



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

NPCC REGIONAL STANDARDS COMMITTEE

AGENDA FOR MEETING #21-2

May 12, 2021 12:00 p.m. – 4:00 p.m. EDT **WebEx Meeting**
DER VER Forum May 13, 2021 8:30 a.m. – 2:00 p.m. EDT **WebEx Meeting**

Dial-In: 415-655-0003 (USA) / 416-915-6530 (Canada)

Day 1 - RSC Business:

Guest Code: 1851217290

Password: 6TmsPEtm*64 (68677386 from phone)

[WebEx Link](#)

Day 2 - DER VER Forum:

Guest Code: 1856003526

Password: FWjfb2m2F\$5 (39532262 from phone)

[WebEx Link](#)

For Reference:

[Glossary of Terms Used in NERC Reliability Standards](#), dated January 4, 2021

[NPCC Glossary of Terms](#), dated October 2, 2019

Introductions and Chair's Remarks- COVID-19, NERC and FERC

NPCC Antitrust Compliance Guidelines

Agenda Items:

1.0 Review of Agenda

2.0 RSC Meeting Minutes (Approval Item)

3.0 Items Requiring RSC Discussion

3.1 [NPCC DER Guidance Revision](#)

3.2 [FERC Activities](#)

3.3 [NPCC Directory Prioritization Whitepaper](#)

4.0 NERC Reliability Standards

<http://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx>

4.1 Currently Posted Projects

Project	Comment Period End Date	Ballot Period End Date
<u>Project 2016-02 Modifications to CIP Standards</u> Norm Dang from IESO @ 12:15 PM	3/22/21 (F)	3/22/21 (I)
<u>Project 2017-01 Modifications to BAL-003-1.1</u> David Lemmons from Cooper Compliance @ 12:30 PM	4/27/21 (I)	10/24/19 (F)
<u>Project 2019-02 BES Cyber System Information Access Management</u> William Vesely from Con Edison @ 12:45 PM	9/21/20 (F)	5/10/21 (A)

Project 2019-04 Modifications to PRC-005-6 Giannuzzi Giuseppe from HQ @ 1:00 PM	2/26/21 (F)	
Project 2019-06 Cold Weather Matthew Harward @ 1:15 PM	4/26/21 (F)	4/26/21 (A)
Project 2020-02 Transmission-connected Dynamic Reactive Resources Latrice Harkness @ 1:45 PM	3/20/20 (I)	
Project 2020-03 Supply Chain Low Impact Revisions SAR Tony Hall @ 1:30 PM	6/3/20 (I)	
Project 2020-04 Modifications to CIP-012	6/11/20 (I)	
Project 2020-05 Modifications to FAC-001-3 and FAC-002-2 SAR	12/11/20 (I)	
Project 2021-01 Modifications to MOD-025 and PRC-019	4/2/21 (I)	
Project 2021-03 CIP-002 Transmission Owner Control Centers		
Comments: (I) – Informal; (F) – Formal; (N) – Nomination Period Ballots: (I) – Initial; (A) – Additional; (F) – Final		

- 4.2 Ballot History (Since last RSC Meeting)
- 4.3 Comment Form History (Since last RSC Meeting)

5.0 **NPCC Non-Standards**

<https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx>

- 5.1 Items for Discussion
 - 5.1.1 NPCC Goal --- Prioritization of Directory Reviews
 - 5.1.2 Directory#1 Design and Operation of the BPS --- Scope of Work
 - 5.1.3 Directory#12 UFLS --- Retirement
 - 5.1.4 Directory#11 Disturbance Monitoring --- TFSP Review
 - 5.1.5 Executive Tracking Summary

6.0 **RSC Member Items of Interest**

- 6.1 RSC Roster

7.0 **Standards Activity Post NERC BOT Approval**

(Since last RSC Meeting)

- 7.1 NERC Filings to FERC
<http://www.nerc.com/FilingsOrders/Pages/default.aspx>
- 7.2 FERC Orders / Rules
<http://www.nerc.com/FilingsOrders/Pages/default.aspx>
- 7.3 Federal Register
<https://www.federalregister.gov/>
- 7.4 [FERC Sunshine Act Meeting Notice](#)
- 7.5 [FERC Open Meeting Summaries](#)

8.0 **NERC Meetings**

8.1 Standards Committee (SC)

<http://www.nerc.com/comm/SC/Pages/default.aspx>

January 20 th – Call	February 17 th – Call	March 17 th – Call
April 21 st – Call	May 19 th – Call	June 16 th – Denver, CO (Xcel Energy)
July 21 st – Call	August 18 th – Call	September 23 rd – Salt Lake City, UT (WECC)
October 20 th – Call	November 17 th – Call	December 15 th – Atlanta, GA (NERC)

8.2 Board of Trustees (BOT) Meeting

<http://www.nerc.com/gov/bot/Pages/Agenda-Highlights-and-Minutes-.aspx>

February 5-6 - Meeting	May 13-14 - Meeting	August 19-20 – Conference Call
November 4-5 – Conference Call		

9.0 **NERC Items of Interest** (Since last RSC Meeting)

9.1 Lessons Learned

<http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx>

- 9.1.1 There have been seven new Lesson Learned issued since the last RSC meeting.

9.2 Alerts

<http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx>

There has been one new NERC Alerts released since the last RSC meeting.

9.3 NERC Reliability and Security Guidelines

<https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx>

9.4 NERC Rules of Procedure

<https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx>

10.0 **Other Items of Interest**

10.1 NPCC Board of Directors Meeting (BOD) 2021

January 27 th – SGR Law Offices, Jacksonville, FL	March 17 th - Call	May 5 th – NPCC Office
June 2 nd – Call	June 23 rd – NPCC Office	August 4 th – Call
September 1 st and 2 nd – Pierce Atwood	October 27 th – Call	December 1 st – Halifax, NS

11.0 **Future RSC Meetings and Conference Calls**

11.1 RSC 2021 Meeting Dates

February 10 th -11 th , WebEx
May 12 th -13 th , WebEx
August 11 th -12 th Toronto/Montreal or WebEx
October 13 th -14 th Toronto/Montreal or WebEx
December 2 nd General Meeting or WebEx

Day Two RSC Meeting – DER VER Forum:

May 13, 2021 8:30 a.m. – 2:00 p.m. (all times in EDT)

12.0 Distributed Energy Resources (DER) Variable Energy Resources (VER) Forum Topics

- 12.1 Chair Opening Remarks, Antitrust Guidelines, Disclaimer, Public Notice, and Meeting Protocols - Guy V. Zito, NPCC Chair of the RSC and DER Forum (8:30 am - 8:40 am)
- 12.2 FERC Order 2222 Overview – Guy Zito (8:40 am – 8:50 am)
- 12.3 FERC Order 2222 NAESB Standards development – Dick Brooks, Reliable Energy Analytics (8:50 am – 9:00 am)
- 12.4 ISO-NE (9:00 am - 10:15 am)
 - 12.4.1 Addressing How Increasing DER Impacts System Operations – Dean LaForest
 - 12.4.2 FERC Order 2222 – Stephen George
- 12.5 FERC Order 2222 and DER integration R&D needs – Erik Ela and Deepak Ramasubramanian, EPRI (10:15 am - 11:00 am)
- 12.6 DER Aggregation Registration – John Romano, Con Edison (11:00 am – 11:30 am)

15 Minute Break (11:30 am - 11:45 am)

- 12.7 Hilo – Maude Lemieux, Hydro Quebec (11:45 am - 12:30 pm)
- 12.8 Advanced Inverters and Phased Deployment Plan – David Lovelady, National Grid, on behalf of the Joint Utilities of New York (12:30 pm - 1:15 pm)
- 12.9 Blockchain and Energy - Claudio Lima, Enterprise Blockchain, Chair of IEEE Blockchain Working Group (1:15 pm - 1:45 pm)
- 12.10 Discussion, Future Topics and Forums, and Other Matters – Guy Zito, NPCC (1:45 pm - 2:00 pm)

Northeast Power Coordinating Council, Inc. (NPCC)

Antitrust Compliance Guidelines

It is NPCC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. The antitrust laws make it important that meeting participants avoid discussion of topics that could result in charges of anti-competitive behavior, including: restraint of trade and conspiracies to monopolize, unfair or deceptive business acts or practices, price discrimination, division of markets, allocation of production, imposition of boycotts, exclusive dealing arrangements, and any other activity that unreasonably restrains competition.

It is the responsibility of every NPCC participant and employee who may in any way affect NPCC's compliance with the antitrust laws to carry out this commitment.

Participants in NPCC activities (including those participating in its committees, task forces and subgroups) should refrain from discussing the following throughout any meeting or during any breaks (including NPCC meetings, conference calls and informal discussions):

- Industry-related topics considered sensitive or market intelligence in nature that are outside of their committee's scope or assignment, or the published agenda for the meeting;
- Their company's prices for products or services, or prices charged by their competitors;
- Costs, discounts, terms of sale, profit margins or anything else that might affect prices;
- The resale prices their customers should charge for products they sell them;
- Allocating markets, customers, territories or products with their competitors;
- Limiting production;
- Whether or not to deal with any company; and
- Any competitively sensitive information concerning their company or a competitor.

Any decisions or actions by NPCC as a result of such meetings will only be taken in the interest of promoting and maintaining the reliability and adequacy of the bulk power system.

Any NPCC meeting participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NPCC's antitrust compliance policy is implicated in any situation should call NPCC's General Counsel and Corporate Secretary, Kristin McKeown Esq. at her mobile phone number 646-581-0148.

Distributed Energy Resources Forum Disclaimer Statement

1. General

Any information presented [at NPCC forums] is for informational purposes only. NPCC accepts no responsibility for the accuracy of such presentations, or for your reliance on any information contained within the content available through such forums. Discussions represent a wide range of views and interests of the participating individuals and organizations. Statements made during discussions do not necessarily reflect those of NPCC.

2. Vendors

Information presented is for stakeholder informational purposes only and does not imply NPCC's endorsement or approval. NPCC does not promote technology, tools, products, services, or vendors that may be used by entities within the electric industry. Questions or concerns about vendors or the services or products they offer must be directed to the vendor. It is the responsibility of the owner, operator, or the user of the bulk power system to research the services the vendors offer. Those that utilize the services of vendors assume full responsibility for claims directly or indirectly arising thereunder and NPCC is not responsible or liable for any claim or harm, directly or indirectly, that transpires from the use of any information.

Public Announcement

RSC and DER Forum Meetings, WebEx, and Conference calls:

Participants are reminded that this meeting, WebEx, and conference call are public. The access number was posted on the NPCC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

NPCC REGIONAL STANDARDS COMMITTEE

AGENDA FOR MEETING #21-1

February 10, 2021 12:00 p.m. – 4:00 p.m. EDT **WebEx Meeting**
DER Forum February 11, 2021 8:00 a.m. – 2:00 p.m. EDT **WebEx Meeting**

Dial-In: 415-655-0003 (USA) / 416-915-6530 (Canada)

Day 1 - RSC Business:

Guest Code: 1783851368

Password: 3iSSaFjc@67 (34772352 from phones)

[WebEx Link](#)

Day 2 - DER Forum:

Guest Code: 1787258377

Password: E8Dn4xfnX@3 (38364936 from phones)

[WebEx Link](#)

For Reference:

[Glossary of Terms Used in NERC Reliability Standards](#), dated January 4, 2021

[NPCC Glossary of Terms](#), dated October 2, 2019

Attendance:

	Name	Organization	Sector(s)	Day(s)
1.	Guy Zito	Northeast Power Coordinating Council		1
2.	Gerry Dunbar	Northeast Power Coordinating Council		1
3.	Ruida Shu	Northeast Power Coordinating Council		1
4.	Kal Ayoub	FERC	Guest	1
5.	Allen Schriver	Proxy for NextEra Energy	4	1
6.	Avani Pandya	Consolidated Edison Co. of New York, Inc.	4	1
7.	Ben Wu	Orange and Rockland	3	1
8.	Brad Nelson		Guest	1
9.	Brian Robinson	Utility Services, Inc.	5	1
10.	Chantal Mazza	Hydro Quebec	2	1
11.	Constantin Chitescu	Ontario Power Generation	4	1
12.	Cristhian Godoy	Consolidated Edison Co. of New York, Inc.	5	1
13.	Dermot Smyth	Consolidated Edison Co. of New York, Inc.	3	1
14.	Dave Kwan	Ontario Power Generation	4	1
15.	David Burke	Orange and Rockland	3	1
16.	David Kiguel	Independent	7	1
17.	Donald Nelson	Mass DPU	Guest	1
18.	Helen Wang		Guest	1
19.	Herb Schrayshuen	Power Advisors, LLC	Guest	1

20.	Jim Grant	NYISO	2	1
21.	Jim Ogle		Guest	1
22.	Joel Charlebois	AESI, Inc.	7	1
23.	John Pearson	ISO-NE	2	1
24.	Junji Yamaguchi	Hydro Quebec	2	1
25.	Lodie White	FERC	Guest	1
26.	Mike Jones	National Grid	3	1
27.	Mike Ridolfino	Central Hudson Gas and Electric	1	1
28.	Michele Shafer	The United Illuminating Company	1	1
29.	Michele Tondalo	The United Illuminating Company	1	1
30.	Mike Cooke	Ontario Power Generation	4	1
31.	Nick Parrotta	PLM	Guest	1
32.	Paolo D'Alessandro		Guest	1
33.	Payam Farahbakhsh	Hydro One Networks	1	1
34.	Quintin Lee	Eversource	1	1
35.	Quyen Diep		Guest	1
36.	Rob Vance	New Brunswick Power	1	1
37.	Salvatore Spagnolo	NYPA	4	1
38.	Sean Bodkin	Dominion	4	1
39.	Sean Cavote	PSEG	4	1
40.	Timothy Kucey	PSEG	4	1
41.	Vijay Puran	New York State Department of Public Service	6	1
42.	zhengq@coned.com		Guest	1
43.	Dean Laforest	ISO-NE	Guest	1
44.	Norm Dang	IESO	Guest	1
45.	David Lemmons	Cooper Compliance	Guest	1
46.	Latrice Harkness	NERC	Guest	1
47.	Matthew Harward	SPP	Guest	1
48.	Giannuzzi Giuseppe	Hydro Quebec	Guest	1
49.	William Vesely	Consolidated Edison Co. of New York, Inc.	Guest	1

Introductions and Chair's Remarks- COVID-19, NERC and FERC

Guy Zito provided his opening remarks and updated the group on the blockchain.

He discussed the potential applications to sell DER energy using blockchain technology. (All electronic)

He also provided an overview of the DER forum tomorrow.

NPCC Antitrust Compliance Guidelines

The NPCC Antitrust Compliance Guidelines were read by Ruida Shu.

Agenda Items:

1.0 Review of Agenda

Guy Zito provided an update on the COVID-19 situation and reviewed the agenda with the group.

2.0 RSC Meeting Minutes (Approval Item)

Approval of the December 3, 2020 Meeting Minutes - No revision is necessary to the draft RSC meeting minutes that were provided in the agenda package.

Jim Grant made the motion for approval.

Quintin Lee seconded the motion.

The December 3, 2020 meeting minutes were approved.

3.0 Items Requiring RSC Discussion

3.1 NPCC DER Guidance Revision

Guy Zito discussed the plans for the third round of review on the NPCC DER Guidance document.

3.2 FERC Activities

Kal Ayoub presented on the recent FERC activities.

He gave an update on all the recent FERC Orders/NOPRs.

Virtualization, Cloud Services for Power Grid Operations which is an order directed NERC to make the filing by January 1, 2022.

He also reviewed the Transmission Cyber Security Incentives NOPR and ERO Five-Year Performance Assessment with the group.

3.3 NPCC 2021 Corporate Reliability Goals

Guy Zito reviewed the NPCC 2021 Corporate Reliability Goals with the RSC members. He focused his discussion on the standards program area and DER.

4.0 NERC Reliability Standards

<http://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx>

4.1 Currently Posted Projects

Project	Comment Period End Date	Ballot Period End Date
Project 2015-09 Establish and Communicate System Operating Limits Dean Laforest from ISO-NE @ 12:15 PM	12/7/20 (F)	12/7/20 (A)
Project 2016-02 Modifications to CIP Standards Norm Dang from IESO @ 12:30 PM	12/16/19 (F)	4/6/20 (F)
Project 2017-01 Modifications to BAL-003-1.1 David Lemmons from Cooper Compliance @ 12:45 PM	4/17/19 (I)	10/24/19 (F)
Project 2019-02 BES Cyber System Information Access Management William Vesely from Con Edison @ 1:00 PM	9/21/20 (F)	9/21/20 (A)
Project 2019-04 Modifications to PRC-005-6	2/26/21	

Giannuzzi Giuseppe from HQ @ 1:15 PM	(F)	
Project 2019-06 Cold Weather Matthew Harward @ 1:30 PM	3/12/21 (F)	3/12/21 (I)
Technical Rationale for Reliability Standards Project is on hold	4/20/20 (I)	4/20/20 (I)
Project 2020-02 Transmission-connected Dynamic Reactive Resources Latrice Harkness @ 1:45 PM	5/13/20 (I)	
Project 2020-03 Supply Chain Low Impact Revisions SAR	6/3/20 (I)	
Project 2020-04 Modifications to CIP-012	6/11/20 (I)	
Project 2020-05 Modifications to FAC-001-3 and FAC-002-2 SAR	12/11/20 (I)	
Project 2020-06 Verifications of Models and Data for Generators SAR	1/14/21 (I)	
Comments: (I) – Informal; (F) – Formal; (N) – Nomination Period		
Ballots: (I) – Initial; (A) – Additional; (F) – Final		

Project 2015-09 Establish and Communicate System Operating Limits:

The SDT will post a revised FAC-014 in late February 2021.

The SDT plans to post the whole package in May 2021.

Project 2016-02 Modifications to CIP Standards:

Project 2016-02 SDT will continue to interface the Project 2019-02 SDT (BCSI in Cloud) that is revising CIP-004-7 and CIP-011-3.

CIP-002-6 proposed changes to criterion designating BES Cyber Systems at certain Control Centers as medium impact.

It is adopted by NERC BOT on May 14, 2020 and filed with FERC on June 12, 2020.

Recent cybersecurity events prompt NERC Staff to gather more data prior to permitting more BES Cyber Systems to become low impact.

CIP-002-6 withdrawn at the Feb 4, 2021, NERC BOT Meeting.

It is likely that a future SDT will be created to look at the proposed changes.

Project 2016-02 SDT is currently posted for a 45-day formal comment period and ballot from January 21 – March 22, 2021.

The plans to post for a second and third 45-day formal comment period with ballot later this year.

The plan is to file for board adoption on November 4, 2021.

Project 2017-01 Modifications to BAL-003-1.1:

David Lemmons called in at 12:44 PM.

The whitepaper for this project is ready for posting and NERC is holding the posting, so they don't overload the industry with projects.

What's in the white paper:

Frequency responses are suggested for more entities such as generators.

Do we want to have a generator requirement?

The SDT is looking for feedback from the industry.

The individual frequency response difference is minor. (2 KW from a 180 MW unit)

The plan is to post the whitepaper for this project towards the end of the CIP project comment period.

Project 2019-06 Cold Weather:

Matthew Harward called in at 12:50 PM.

The project is posted for the first round of comments.

IRO and TOP standards will address data specification requirements for the RC and TOP.

The drafting team can't provide a set term for "cold weather" due to the differences in regions.

The comment period ends March 12, 2021, which is also the initial ballot period opens.

The drafting team plans to host an industry webinar.

Project 2019-04 Modifications to PRC-005-6:

The SDT held an industry webinar last week on this project.

Please submit your comments prior to February 26, 2021.

Only DC batteries for protection systems are included in PRC-005-6.

They want to make it technology agnostic and not limit it to one technology.

Project 2020-02:

SAR is on hold.

Project 2020-03:

SAR drafting team made modifications to the SAR.

SAR is sent to the standard committee and the plans to task the SAR drafting team to be the drafting team.

Project 2020-04:

The project will be posted for late March 2021.

The SAR drafting team will be appointed to be on the SDT.

Project 2020-05:

The SAR is also being reviewed at the next SC meeting for approval.

Project 2020-06:

Project 2020-02 Transmission-connected Dynamic Reactive Resources SAR was posted from March 30 to May 13, 2020, and members of a SAR DT were solicited.

However, Project 2020-02 was paused indefinitely, and a SAR DT was not appointed.

Subsequently, a second SAR involving similar standards, namely MOD-026 and MOD-027 was being drafted by the IRPTF and approved for posting in September 2020 by the Standards Committee.

The Project 2020-06 Verifications of Models and Data for Generators SAR will be posted for industry comment, and additional nominees with MOD-026/027 background will be sought. A single SAR DT will be charged with determining whether to combine the two projects and drafting a combined SAR.

Project 2019-02:

There will be some staggering posting.

Virtualization project 2016-02 first then late March 2021 the BCSI Project 2019-02 team will post.

The goal is to post a calendar that shows all the project posting with their associated standards.
The last ballot did not pass for this project.

The SDT drafted some new language “provision access” and language involves storage units.
The plan is to have the project completed by the end of the year.

The project is in a holding position due to Project 2016-02.

The industry webinar is being delayed from February 2021 to April 2021.

The webinar will be interactive with the industry SMEs.

Three different options:

1. Revised the proposed language from the last posting.
2. Expand on requirement 1.1, have control over the information.
3. Adopt a CIP-012 language.

There is a possibility that NERC will put together another drafting team to work on the CIP standards.

There are concerns about the destruction on the devices that contain sensitive information.

- 4.2 Ballot History (Since last RSC Meeting)
Ruida Shu reviewed the Ballot History document in the meeting.
- 4.3 Comment Form History (Since last RSC Meeting)
Ruida Shu reviewed the Comment Form History document in the meeting.

5.0 NPCC Non-Standards

<https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx>

5.1 Items for Discussion

5.1.1 Directory#7 Approved.

Directory#7 Remedial Action Schemes approved by the Full Members on December 22, 2020.

5.1.2 Directory#1 Design and Operation of the BPS --- Review

Directory#1 TFCO and TFCP developing Scope of Work in advance of 2021 document review.

5.1.3 Directory#12 UFLS --- Retirement

TFSS will consider retirement proposal in 2021.

5.1.4 Executive Tracking Summary

6.0 RSC Member Items of Interest

6.1 RSC Roster

7.0 Standards Activity Post NERC BOT Approval

(Since last RSC Meeting)

7.1 NERC Filings to FERC

<http://www.nerc.com/FilingsOrders/Pages/default.aspx>

7.2 FERC Orders / Rules

<http://www.nerc.com/FilingsOrders/Pages/default.aspx>

7.3 Federal Register

<https://www.federalregister.gov/>

7.4 FERC Sunshine Act Meeting Notice

7.5 FERC Open Meeting Summaries

8.0 NERC Meetings

8.1 Standards Committee (SC)

<http://www.nerc.com/comm/SC/Pages/default.aspx>

January 20 th – Call	February 17 th – Call	March 17 th – Call
April 21 st – Call	May 19 th – Call	June 16 th – Denver, CO (Xcel Energy)
July 21 st – Call	August 18 th – Call	September 23 rd – Salt Lake City, UT (WECC)
October 20 th – Call	November 17 th – Call	December 15 th – Atlanta, GA (NERC)

8.2 Board of Trustees (BOT) Meeting

<http://www.nerc.com/gov/bot/Pages/Agenda-Highlights-and-Minutes-.aspx>

February 5-6 - Meeting	May 13-14 - Meeting	August 19-20 – Conference Call
November 4-5 – Conference Call		

9.0 NERC Items of Interest (Since last RSC Meeting)

9.1 Lessons Learned

<http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx>

9.1.1 There has been no new Lesson Learned issued since the last RSC meeting.

9.2 Alerts

<http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx>

There has been one new NERC Alerts released since the last RSC meeting.

9.3 NERC Reliability and Security Guidelines

<https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx>

9.4 NERC Rules of Procedure

<https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx>

10.0 Other Items of Interest

10.1 NPCC Board of Directors Meeting (BOD) 2021

January 27 th – SGR Law Offices, Jacksonville, FL	March 17 th - Call	May 5 th – NPCC Office
June 2 nd – Call	June 23 rd – NPCC Office	August 4 th – Call
September 1 st and 2 nd – Pierce Atwood	October 27 th – Call	December 1 st – Halifax, NS

10.2 NPCC 2021 Business Plan and Budget Schedule

10.3 Idaho National Labs – Communications – Brad Nelson

11.0 Future RSC Meetings and Conference Calls

11.1 RSC 2021 Meeting Dates

February 10 th -11 th , NYC or WebEx
May 12 th -13 th , WebEx
August 11 th -12 th Toronto/Montreal or WebEx
October 13 th -14 th Toronto/Montreal or WebEx
December 9 th General Meeting or WebEx

Meeting adjourned at 2:18PM.

Day Two DER Forum:

February 11, 2021 8:00 a.m. – 2:00 p.m. EDT

	Name	Organization	Comments
1	Aaron Anaya		
2	Adarsh Nagarajan		
3	Aditya Menon		
4	Al McMeekin	NERC	
5	Alexandre Bellemare		
6	Alexandru Majeru		
7	Allen Schriver	NextEra Energy, LLC	
8	Andre Savidon		
9	Andreas Klaube	NPCC	
10	Andrew Kimball		
11	Andrey Oks	NPCC	
12	Andy Hoke	NREL	
13	Anie Philip	LIPA	
14	Anthony Gorgone		
15	Avani Pandya	Con-Edison	
16	Behzad Sedaghat		
17	Ben Wu	Orange and Rockland	
18	Benjamin Loebick	Orange and Rockland	
19	Brad Fiander		
20	Brad Marszalkowski	ISO-NE	
21	Brad Nelson		
22	Brent Oberlin		
23	Brett Feldman		
24	Brian Evans-Mongeon	Utility Services	
25	Brian Ritzinger		
26	Brian Robinson	Utility Services	
27	Bruce Jagolinzer		
28	Bryan Clark		
29	Call-in User 11		
30	Call-in User 14		
31	Caron Mich		
32	Casey Darling		
33	Catherine Ethier		
34	Chakrapani Venugopalan		
35	Charles Yeung		
36	Chris Overberg	Con-Edison	
37	Christian Fehrenbacher		
38	Christian Garneau		
39	Claudio		

40	Chuck Victor		
41	Constantin Chitescu	OPG	
42	Craig Laffey		
43	Cristhian Godoy	Con-Edison	
44	Dan Kopin	Utility Services	
45	Dan Roethemeyer		
46	Daren V		
47	Dave Conroy	CMPCO	
48	David Mueller		
49	Dhaval Patel		
50	Dianlong Wang		
51	Don Urban		
52	Donald E Nelson	Mass DPU	
53	Dorothy Capra		
54	Dylan Dreisch		
55	Elvin		
56	Evan Margolis		
57	Evan Shuvo		
58	Ganesh Narine		
59	Gerard Dunbar	NPCC	
60	German Encalada		
61	Greg Young-Morris		
62	Guy Zito	NPCC	
63	Hao Fu		
64	Helen Wang		
65	Holden Mann		
66	Hung Huynh		
67	Jack DiOdoardo		
68	James Grant	NY-ISO	
69	James Mcnamara		
70	James Murphy		
71	James Oddy		
72	Jason Pause	NYDPS	
73	Jeff Carrara		
74	Jill Loewer	Utility Services	
75	Jim Ogle		
76	Jim Watson		
77	Joe Farella		
78	John Baudanza		
79	John Koziatek		
80	John Norden		
81	John Pearson	ISO-NE	
82	John Penaranda		
83	John Wang		
84	John Slocum		

85	Joseph Marranca		
86	Judianne O'Brien		
87	Junji Yamaguchi	Hydro Quebec	
88	Keith Lee		
89	Ken Stell		
90	Kevin Clark		
91	Klearko Goro		
92	Kyle Hughes		
93	Lauren Bergman		
94	Lodie White	FERC	
95	Lori Mofford		
96	Marc Allen		
97	Maria		
98	Marie Faber Frolich	Orsted	
99	Mark Gaines		
100	Matei Burlea		
101	Mazza, Chantal	Hydro Quebec	
102	Melinda Montgomery		
103	Michael DelCasale		
104	Michael Jones	National Grid	
105	Michael Lombardi	NPCC	
106	Michael Ridolfino	Central Hudson Gas & Electric	
107	Michele Shafer	Avangrid	
108	Michele Tondalo	Avangrid	
109	Mike Cooke	OPG	
110	Mohamed ElNozahy		
111	Muhammad Ibraheem		
112	Neeraj Lal	NPCC	
113	Nicholas Culpepper		
114	Nick Parrotta	PLM	
115	Nicola Montanaro		
116	Nicolas Compas	Hydro Quebec	
117	Ovidiu Vasilachi		
118	Paolo D'Alessandro		
119	Paul DiFilippo		
120	Paul MacDonald		
121	Payam Farahbakhsh	Hydro One	
122	Per-Anders Lof	National Grid	
123	Peter McEleney		
124	Phillip Woo		
125	Quintin Lee	Eversource	
126	Quyen Diep		
127	Rafael Sahiholamal	NPCC	
128	Randy Crissman	NYPA	
129	Ray Mason		

130	Reigh Walling	Contractor	
131	Rizki Del Olmo		
132	Rob Vance	NBPower	
133	Robert Eisenhuth		
134	Roberto Reyes		
135	Roger Clayton	NYSRC	
136	Rudi Vega		
137	Ruida Shu	NPCC	
138	Salvatore Spagnolo	NYPA	
139	Sean Cavote	PSEG	
140	Shayan Rizvi	NPCC	
141	Sheila Keane		
142	Slawek Szymanowski		
143	Sophie Giner		
144	Stephen Capozzi		
145	Steven Bruckner		
146	Swagata Sharma		
147	Thinh Pham		
148	Tim Miller		
149	Tom Burns		
150	Tom Muratore		
151	Tony Napikoski UI	UI	
152	Tracy MacNicol	Utility Services	
153	Trupti		
154	Troels Stybe Soerensen		
155	Umair Hanif		
156	Veronica Mendes		
157	Vijay Puran	NYSDPS	
158	Wayne Sipperly	NAGF	
159	William Vesely	Con-Edison	
160	Xiaoyuan Fan		
161	Yujie Lu		
162	Yves Albert		
163	Zhu, Chuanjiang Chelsea		
164	Zoraini Rodriguez		

12.0 Distributed Energy Resources (DER) Forum Topics

- 12.1 Chair Opening Remarks, Antitrust Guidelines, Meeting Protocols - Guy V. Zito, NPCC Chair of the RSC and DER Forum (8:00 am – 8:10 am)
Mr. Zito opened the DER forum by welcoming the attendees and reviewing the agenda.
Mr. Zito provided brief opening remarks that addressed NPCC's role in standard development, its regional criteria, and the impact of distribution system DER and VER on the reliable operation of the BES.
Mr. Zito advised the attendees that the DER forum was open to the public and will be recorded.
- 12.2 Offshore Wind Protection System Philosophy presentation by Marie Faber Frølich/ Behzad Sedaghat from Orsted, Denmark (8:10 am - 9:00 am)
Ms. Frolich provided an overview of protection and control concerns in offshore wind farms. Orsted is the world's largest developer of Offshore Wind Power, with numerous facilities either already in service or in development in North America. Ms. Frolich and Mr. Sedaghat summarized several technical challenges including: 1) Directional elements in protection relays, 2) Zero miss a common phenomenon during cable energization 3) Voltage support and stability during fault conditions including negative sequence fault contribution.
- 12.3 TFSP System Protection presentation by Anthony Napikoski from UI/NPCC TFSP Chair (9:00 am - 9:30 am)
Mr. Napikoski provided background on the work of NPCC's Task Force on System Protection and on protection and control issues related to the installation of DER. Mr. Napikoski highlighted short circuit modelling concerns related to the installation of DER and challenges associated with UFLS.
Mr. Napikoski stated that the growth of DER will requires changes to protection design and modelling.

- 12.4 Advanced Inverter Functions - IEEE 1547-2018 and the testing standard 1547-2020 presentation by Andy Hoke from NREL (9:30 am - 10:15 am)
Mr. Hoke provided background on the development and status of relevant IEEE Standards including IEEE 1547-2018 and IEEE P2800.
Mr. Hoke described the paradigm shift in IEEE 1547-2018 and the ongoing work on IEEE P2800 which is about to enter ballot.
Mr. Hoke also described other planning and operating challenges related to DER including testing, verification, and communication.
- 12.5 PRECISE – a distribution optimizing tool for DER to determine settings for inverters - Adarsh Nagarajan from NREL (10:15 am - 11:00 am)
Mr. Nagarajan provided background on various ways that DER can provide support to the power grid including voltage and frequency support.
Mr. Nagarajan provided details on a case study in Hawaii where technical challenges related to the installation of DER were studied.
Mr. Nagarajan also described a distribution optimizing tool that enables support from solar installations with advanced inverters. PRECISE works with all sizes of solar installations, needs no communication infrastructure and helps maximize full solar capability.

Break for 15 minutes

- 12.6 Blackstart using inverter - based resources presentation by Himanshu Jain from NREL (11:15 am - 12:00 pm)
Mr. Jain from National Renewable Energy Laboratory Nagarajan described current research associated with black start capability from Inverter Based Resources (IBR).
Mr. Jain noted that while black start from IBR is technically feasible there are many unknowns and research is just underway.
Mr. Jain described grid forming to model the constraints of the actual power system, modelling validation and simulations for feasibility and the development of business models to assign value to the capability.
- 12.7 Harmonics and power quality presentation by David R. Mueller from EnerNex (12:00 pm - 12:45 pm)
Mr. Mueller presented on wind and solar IBR and the relevant IEEE Standards on Harmonics.
Mr. Mueller provided general background on the concept of harmonics, and also described other issues associated with power quality and harmonics including, wind and solar inverter characteristics, the requirements of IEEE Standard 519, resonance

considerations, additional background on IEEE 1547 and IEEE 2800 and modelling considerations.

- 12.8 NERC SPIDERWG Updates and NERC IRPWG Battery Energy Storage System and Hybrid Plant Guideline presentation by Ryan Quint (12:45 pm – 1:30 pm)
Mr. Quint provided an update on current activities at NERC.
Mr. Quint provided background on the work of the System Planning Impacts of Distributed Energy Resources (SPIDER) Working Group and the Inverter Based Resource Performance Working Group (IRPWG).
Mr. Quint also summarized a guideline currently under development for the performance, modelling and simulations of BPS connected Battery Energy Storage Systems and Hybrid Power Plants.
- 12.9 ISO-NE Proposed Changes to ISO-SRD presentation by Brad Marszalkowski
Mr. Marszalkowski summarized proposed changes to the ISO-NE SRD (Source Requirements Document).
Mr. Marszalkowski provided background and details on the draft changes to the SRD including the addition of requirements for non-inverter-based units, rate of change of frequency (ROCOF) requirements, return to service requirements and complete compliance with IEEE 1547-2018.
- 12.10 NPCC DER Guidance Document and Chair Closing Remarks – Guy V Zito, NPCC Chair of the RSC and DER Forum (1:30 pm – 2:00 pm)
Mr. Zito thanked all the participants for their timely and informative presentations.
Mr. Zito summarized anticipated RSC DER and VER activities during 2021 including, further collaboration with state and provincial regulators, a review of NPCC documents and criteria to prioritize their review, expansion of the current DER forum format to include VER facilities connected to the transmission system and any other issues not addressed by NERC.
Mr. Zito thanked the attendees and presenters once more and adjourned the DER forum.

Northeast Power Coordinating Council, Inc. (NPCC)

Antitrust Compliance Guidelines

It is NPCC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. The antitrust laws make it important that meeting participants avoid discussion of topics that could result in charges of anti-competitive behavior, including: restraint of trade and conspiracies to monopolize, unfair or deceptive business acts or practices, price discrimination, division of markets, allocation of production, imposition of boycotts, exclusive dealing arrangements, and any other activity that unreasonably restrains competition.

It is the responsibility of every NPCC participant and employee who may in any way affect NPCC's compliance with the antitrust laws to carry out this commitment.

Participants in NPCC activities (including those participating in its committees, task forces and subgroups) should refrain from discussing the following throughout any meeting or during any breaks (including NPCC meetings, conference calls and informal discussions):

- Industry-related topics considered sensitive or market intelligence in nature that are outside of their committee's scope or assignment, or the published agenda for the meeting;
- Their company's prices for products or services, or prices charged by their competitors;
- Costs, discounts, terms of sale, profit margins or anything else that might affect prices;
- The resale prices their customers should charge for products they sell them;
- Allocating markets, customers, territories or products with their competitors;
- Limiting production;
- Whether or not to deal with any company; and
- Any competitively sensitive information concerning their company or a competitor.

Any decisions or actions by NPCC as a result of such meetings will only be taken in the interest of promoting and maintaining the reliability and adequacy of the bulk power system.

Any NPCC meeting participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NPCC's antitrust compliance policy is implicated in any situation should call NPCC's Assistant Secretary, Ruta Skučas, Esq. at 1-202-530-6428.

Public Announcement

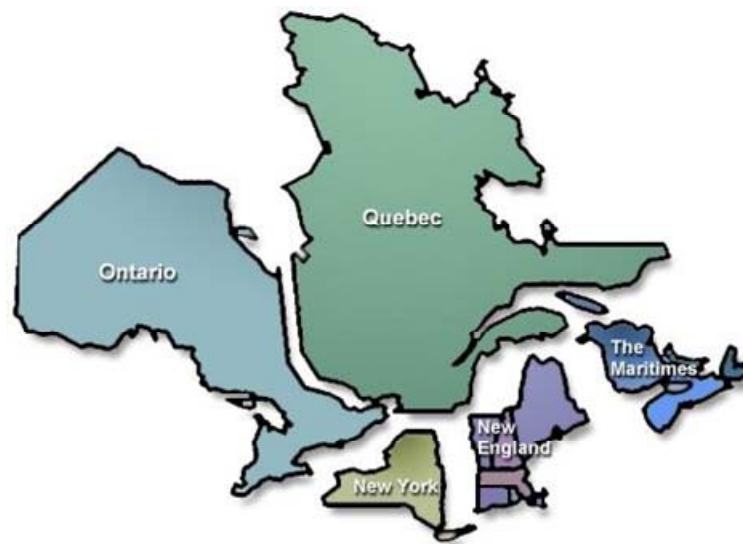
RSC and DER Forum Meetings, WebEx, and Conference calls:

Participants are reminded that this meeting, WebEx, and conference call are public. The access number was posted on the NPCC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

NPCC DER Guidance Document, Distributed Energy Resources (DER) Considerations to Optimize and Enhance System Resilience and Reliability



NPCC Regional Standards Committee (RSC)
Version 2 Approved 11/20/2020

Note: Content of this document may not reflect the most current information¹. Periodic reviews for potential revisions of the document will be done biannually or more frequently if needed. Please send corrections or revision requests to npccstandard@npcc.org.

Contributors:

Jens Boemer	Electric Power Research Institute (EPRI)
David Conroy	Joint Utilities of New York-CMP
David Forrest	EPRI Consultant
James Grant	NYISO
Michael Jones	National Grid (RSC Co-Vice Chair)
Dan Kopin	Utility Services
Benjamin Kroposki	National Renewable Energy Lab (NREL)
Quintin Lee	Eversource (RSC Co-Vice Chair)
Benjamin Loebick	United Illuminating
Brad Marszalkowski	ISO-NE
John Pearson	ISO-NE
Ryan Quint	NERC
Brian Robinson	Utility Services
Herb Schrayshuen	Power Advisors, LLC
Reigh Walling	Walling Energy Systems Consulting, LLC
Guy V. Zito	NPCC (RSC Chair)

NPCC also thanks the Regional Standards Committee (RSC) and the State and Provincial regulatory authorities who provided guidance and information during the development of this document.

Revision History

Version	Date	Action	Change Tracking (New, Errata or Revisions)
1	8/19/19	Effective Date	New
2	X/XX/XX	RSC and Subgroup developed revisions	Revisions, add AGIR, new title, clarifications, and Appendices

¹ The guidance provided in this document is not mandatory, makes no warranty or representations, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in the Material. Additionally, NPCC assumes no liability with respect to the use of, or for damages resulting from, the use of the Material.

Contents

Executive Summary.....	5
Introduction and Objective	6
NPCC DER Impact Reporting	8
DER BPS Impact Considerations.....	9
NPCC Interconnection Guidance.....	9
Voltage Response.....	12
Frequency Support.....	13
Reconnection to the Utility System	14
Inverters	14
Certification per UL 1741 SA and UL 1741 SB as grid support utility interactive inverters	16
Protective Functions	16
Metering	18
Power Quality.....	19
Power Factor	20
Islanding	20
Automatic Underfrequency Load Shedding (UFLS) Programs	20
Effective Grounding for DER	21
Resource Adequacy.....	22
Energy Storage Systems for DER.....	22
System Control and Data Acquisition (SCADA) and Communications.....	23
DER Recommendations.....	25
Appendix A, NPCC DER Impact Reporting Form and Process	28
Appendix B, NPCC Areas- Comparisons	30
Appendix C – SPIDER Working Group Reliability Guidelines & Activities	31
Appendix D, NPCC Reliability Principles.....	34
Appendix E, State and Provincial AGIR Information	37
New York State.....	37
New England, by State	37
Province of Quebec (some references are only available in French)	40
Province of Ontario	43
Province of New Brunswick	44
Appendix F, ISO New England	45

Appendix G, State Renewable and Green Energy Targets.....	47
Appendix H, Autonomous Energy Grids.....	48

Executive Summary

The Northeast Power Coordinating Council, Inc. (NPCC) is responsible for promoting and enhancing the reliability of the International, interconnected Bulk Power System in Northeastern North America.

Development of this document was initiated by the NPCC Board of Directors to provide regional guidance and information for voluntary use by NPCC Members and stakeholders. The guidance provided herein identifies potential reliability risks² to the Bulk Power Systems (BPS), recommendations to mitigate them, and also identifies opportunities to optimize the operational characteristics of DER to enhance reliability and resilience of the NPCC Bulk Power System (BPS). The document outlines both existing DER deployment practices and strategies as well as how a future with increased penetration of DER and internet controllable devices could be reliably coordinated ([Appendix H](#)). Links to other resources have also been provided throughout the document.

As Distributed Energy Resources (DER) continue to replace traditional industry generation resources the resource fuel mix and operational characteristics of the system will change. DER will necessitate changes to how the system is planned and operated. The North American Electric Reliability Corporation (NERC) Reliability Standards are not applicable to equipment on the distribution systems unless such equipment has a direct impact on the “reliable operation”³ of the BPS, such as Automatic Underfrequency Load Shedding (UFLS). However, as penetration of DER increases, planning and operating assessments used to assure reliable operation of the BPS will need to accurately represent how DER interacts with the BPS.

NPCC recognizes that continent-wide efforts in North America are underway at the NERC level to define DER and address some aspects related to planning and modeling. [Appendix C](#) outlines some specific reliability activities related to DER which have either been developed, or are in the process of being developed, by the NERC System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG), along with links to some of their documents. NPCC and its members have also been engaged in the work efforts at the NERC level and are leading efforts to address outstanding issues within the scope of those groups and provide expertise. With the understanding of all the efforts which are underway, NPCC can coordinate and fill a vital role in identifying additional areas where the Region may provide information and services to promote reliable deployment of DER. An example is coordination with State and Provincial Government Regulatory Authorities, and distribution utilities. Also, opportunities exist in the areas of obtaining data, models, testing and verification, observability, protection systems and other operational characteristics of DER and their effect on the distribution systems.

² An example of a reliability risk not addressed is remote dispatch of DER. A significant challenge that has been found by some NPCC members is that DER Operators can be anywhere in the world and that as a result, communications can be significantly delayed, leading to reliability risks. This includes time zone challenges and language challenges,

³ “reliable operation” is defined in 16 U.S. Code § 824o and means “operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.”

NPCC has also been conducting DER Forums, the purpose of which is to promulgate DER related information, educate, and inform. NPCC's Regional Standards Committee (RSC) and Reliability Coordinating Committee (RCC) have also developed a joint process and a form to report DER related impacts (i.e. during or following an event both enhancing reliability or causing a reliability risk) and analyze and determine if any further actions are needed. The Form and process may be found in [Appendix A](#) and on the NPCC website.

NPCC is not creating new Criteria or Standards through this guidance document. The intent of this document is informational and as NERC's SPIDERWG, and other groups develop their respective guidance documents it will be revised to achieve continued alignment and avoid duplication.

This guidance document contains [DER Recommendations](#), and information provided by NPCC's Members, NERC, the industry, the US National Renewable Energy Labs, the Electric Power Research Institute (EPRI) and information from NPCC Staff. Also, it is important to note that specific distribution utility requirements within NPCC at the local level will supersede any suggested approaches in this document.

Introduction and Objective

A consistent defined term for what type of generating, demand or storage resources are included in DER is not broadly accepted by industry stakeholders. Also, DER is not currently a term that is defined by NERC.

For the purpose of this NPCC guidance document, DER refers to:

Any non-BPS connected real or reactive power resources (generating units, multiple generating units at a single location, distributed generation installations, battery storage systems, etc.) located within the boundary of any distribution utility's service territory, regardless of capacity, allowing individual DER to be captured if they are not aggregated. Some DER technologies are more intermittent in their production characteristics than resources which operate based on a controllable fuel input.

Initially, in the first version of this guidance document, NPCC specified a threshold for inclusion of DER in any regional guidance that would not include individual rooftop solar or individual wind turbines or other DER net metering installations. However, the aggregate effect of these types of DER can have a significant effect on the power system and if not properly understood can impact the reliable operation of the BPS, as we have seen in California subsequent to their Rule 21⁴. NPCC is now beginning to observe aggregations of DER entering into the capacity wholesale markets within the NPCC Region. This

⁴ <https://www.cpuc.ca.gov/Rule21/> Electric Rule 21 is a tariff that describes the interconnection, operating and metering requirements for generation facilities to be connected to a California utility's distribution system. The tariff provides customers wishing to install generating or storage facilities on their premises with access to the electric grid while protecting the safety and reliability of the distribution and transmission systems at the local and system levels.

document will continue to be modified as emerging issues related to DER's deployment, interconnection, planning and operations are identified and technology improves.

This document identifies opportunities for DER related process improvements and addresses potential reliability risks, promotes good utility interconnection practices necessary for reliability, and promulgates information on how DER can enhance reliable operation at the Transmission Distribution interface by providing essential reliability services. In addition, during the development of this document, a review of existing DER related documents was performed and NPCC is working with the NY Interconnection Technical Working Group (ITWG) as well as the Joint Utilities group of NY to align processes where possible. As other related groups and endeavors are identified within the Region, NPCC will monitor and review their activities going forward and will coordinate with the NPCC Areas and its Members, as necessary.

International standards are established to address DER impact on system reliability. IEEE 1547-2018 as amended by IEEE 1547a-2020 brings significant potential benefits to the BPS by requiring that DER provide essential reliability services to ensure stability, reliability, and security. State and Provincial requirements for DER interconnection should also require compliance with IEEE 1547-2018 through inclusion in their respective jurisdictional interconnection agreements.

As DER continues to proliferate on the electric system at the "grid edge" or distribution system, and replace conventional transmission grid connected resources, there is an increasing reliability related need to understand the effect of DER resources on the BPS. It is important to understand how DER is interconnected, planned, operated and how DER interacts with the transmission system.

Reliably and securely integrating DER into the electric system requires a comprehensive multi-pronged approach utilizing perspectives from different disciplines. DER design, modeling, planning, and relay coordination require consideration of jurisdictional issues. The importance of Members working with their respective national, state, and provincial regulatory authorities to help them understand the consequences of and the development of effective DER interconnection requirements is critical. While there may be some broad universal guidelines, the details of effective DER interconnection requirements should be reconciled with the characteristics of the system where the interconnection is taking place. [Appendix B](#) of this document provides a comparison of NPCC's Area requirements, at the time of the Version 1 writing, to help identify opportunities for guidance.

Many, if not most, of the current DER being deployed is theoretically capable of bringing several enhancements to reliability, provided that there are sufficient design specifications and interconnection requirements to implement the benefits. Inverter based DER may use fast, programmable responses to provide benefits to reliability if properly configured and coordinated with the host utility. Coordination must consider effects both on the distribution system and the BPS. The sections below address DER impact on the BPS including aspects of:

- Interconnection guidance
- Voltage response
- Frequency support

- Reconnecting to the utility following faults
- Underfrequency load shedding

While DER presents opportunities to enhance reliability, they also introduce challenges at the Transmission Distribution interface if not deployed correctly. Interoperability with the transmission system is not solely determined at the point of interconnection. Visibility and a level of controllability of DER is essential for transmission operators to maintain situational awareness for reliable operation of the BPS, and for short-term forecasting. Additionally, characteristics of DER such as capacity, intermittent production, location, protection settings, and other parameters must be known for long-term operational performance forecasting and system planning to ensure BPS reliability is maintained. Additionally, the local distribution utility overseeing the interconnection of DER needs to be able to ensure that the DER doesn't cause safety issues for distribution line workers.

Presently there are limited study tools in general use to perform fully integrated studies of transmission and distribution which would allow both systems to be modeled and studied (in steady-state and dynamically) together, although work is underway in this regard. In the shorter term, visibility of the variability of DER capacity could dramatically affect the quality of state estimator information, and methods of improving data and forecasting need to be explored. The U.S. Department of Energy Argonne National Laboratory has a project underway to develop a tool that would Co-simulate Transmission and Distribution systems. The tool being developed will utilize Siemen's Power System Simulator "PSS®E" transmission system analysis tool with EPRI's open sourced distribution system smart grid tool "OpenDSS"([Smart Grid Simulation Tool](#)) using a Python interface. A detailed presentation on this project may be found in the October 2019 NPCC DER Forum meeting materials on NPCC's website. Additionally, some planners in the NPCC Region are moving to composite load models for their simulations and planning activities.

In recognition of both the benefits and challenges associated with DER, the approach taken with this second version of the NPCC DER Guidance Document is to continue to collect interconnection related information within the NPCC Region as well as in other areas of the NERC Electric Reliability Organization (ERO) Enterprise. There are some specific situations where opportunity exists to ensure better coordination across the NPCC Region. The intent of this document is to identify any emerging reliability issues, provide general guidance and information where possible, and offer support to NERC and others North America wide to promote reliable interconnection and operation practices for DER. It is also recognized that DER may not be located optimally and/or in areas where deliverability to load may not be ideal. In this respect any specific information in this document must be considered in conjunction with the requirements of the interconnecting distribution utility.

NPCC DER Impact Reporting

In order to ensure the reliability and resilience of the interconnected BPS in Northeastern North America as DER, both aggregated and single installations, continue to proliferate throughout the distribution systems within the NPCC Region, it is important to have a regional DER impact reporting mechanism. The NPCC Regional Standard Committee (RSC) created an impact reporting form and process that allows entities to report DER impacts and to seek guidance regarding emerging issues and reliability risks that

affect or could affect the reliable performance of the BPS (see [Appendix A](#)). The Word version of the form also is available on the NPCC website at:

[BES Impact Reporting Form](#)

Impact reporting and its associated process provide an orderly mechanism for NPCC to review reliability impacts submitted. A Report will initiate a collaborative review by the Reliability Coordinating Committee and the Regional Standards Committee.

DER BPS Impact Considerations

NPCC's Regional Standards Committee (RSC) and Task Forces (i.e. Task Force on System Studies) reviews of DER as it pertains to the NPCC Region's BPS performance have identified several areas which, going forward, may warrant further and continual monitoring and analysis. NPCC has identified the following items that should be carefully considered as DER levels (total MWs) increase.

- DER performance with respect to voltage and frequency ride through
- DER ability to provide regulation and reserves
- DER dispatch and controllability
- DER availability, quality of forecasting, and verification
- Observability and situational awareness of DER, and the importance of implementing Advanced Metering Infrastructure (AMI) if telemetry is not deployed
- DER impacts on Underfrequency Load Shed programs
- Impacts of DER on System Restoration and Black Start Plans

Although DER markets, both wholesale and dual participation models, are not the focus of this document, due consideration should be given to their structure. Market rules that allow aggregation also vary across the NPCC Region. Some Areas allow injection of the aggregation across their market area while other Areas require specific aggregations to be injected nearest to a transmission node. DER are capable of providing ancillary services that are necessary to support reliability, if there are appropriate market mechanisms and incentives that allow and encourage them to do so. Wide-area aggregation and injection may create challenges for the system planners and operators as well as raise deliverability and operations concerns.

NPCC Interconnection Guidance

This document and any detailed specifications which follow, are intended to provide examples of general information regarding DER interconnection. The examples do not constitute a Regional Criteria (which can only be implemented through NPCC Directories and approval of NPCC's Full Members). There are numerous efforts underway in many forums and regulatory bodies that are expected to create new, more specific guidance⁵. The level of detail and specificity provided is intended to be used as

⁵ At the time of this guidance document development, these include but are not limited to: NERC (e.g. SPIDER WG, Inverter- Based Resources Task Force (IRPTF), Events Analysis, Modelling and Standards process), IEEE (IEEE Std

information and guidance for any NPCC Member Area which may not have yet seen the need to establish detailed operating parameters. This document shares the practices of some Members of NPCC which have already established detailed DER requirements, even in advance of upcoming applicable industry standards due to the rate of penetration of DER in their Area. NPCC Members considering improving or adding to their respective DER guidance documents are encouraged to reach out directly to other NPCC Members which may have already addressed DER related reliability risk issues.

NERC and NPCC have criteria for resource and transmission planning. For transmission, criteria require transmission planners to simulate different transmission system events and ensure the transmission system remains reliable by meeting performance characteristics for these events. If the transmission system does not remain reliable, the planners are required to identify remediation, including upgrades or expansions of the transmission system. One aspect of the simulation is to account for the loss of generation resources. If a significant amount of DER trips or ceases to inject current for the simulated transmission event, the transmission system could become unreliable for that event and require remediation. This can occur in several scenarios such as a peak load day with maximum output from DER like solar PV or a light load spring day where PV solar and small hydro make up a significant percentage of the generation. IEEE Std. 1547-2018 “Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power System Interfaces” addresses this issue by setting the default DER trip settings for Category II at a level that coordinates with NERC standard PRC-024-2 “Generator Frequency and Voltage Protective Relay Settings.” This is the standard that defines ride-through capability for generators connected to the transmission system. Requiring DER to ride-through disturbances, similarly to large generators, would be a significant step towards achieving a robust level of reliability in a cost-effective manner.

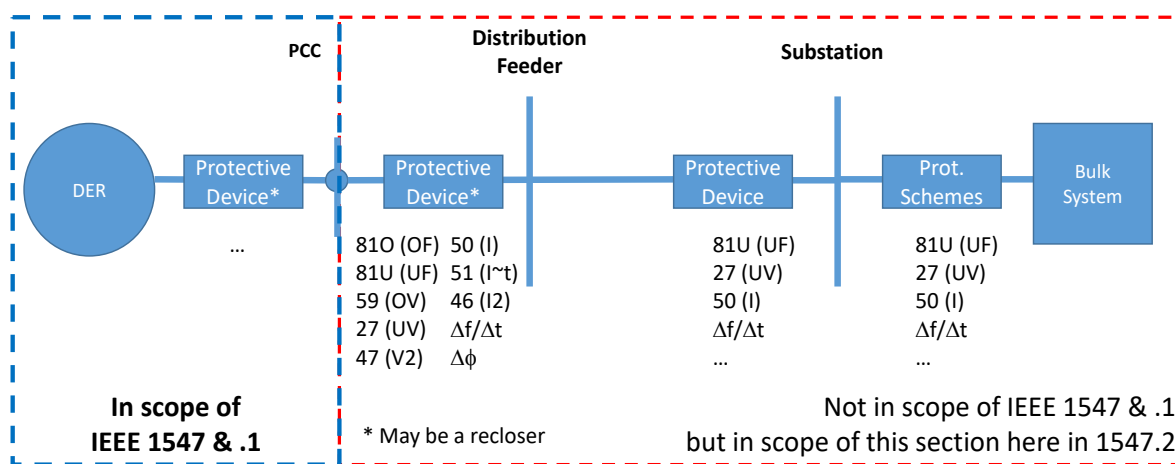


Figure 1: Scope of IEEE 1547 series of standards and guidelines and list of distribution protective functions that may interfere with DER ride-through. Source: Provided courtesy of EPRI⁶

1547.1-2020, P2800), and various state initiatives such as the New York Interconnection Technical Working Group (ITWG), Other regional, Provincial and State initiatives.

⁶ EPRI makes no warranty or representations, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in the Material. Additionally, EPRI assumes no liability with respect to the use of, or for damages resulting from the use of the Material.

IEEE 1547-2018 was unanimously adopted by the National Association of Regulatory Utility Commissioners (NARUC) in 2019. The standard outlines the technical specifications and performance requirements which are universally needed for interconnection and interoperability of DER and should be sufficient for most installations. Implementation guidance for IEEE 1547-2018 may be found here: [Guideline IEEE 1547-2018](#). The applicability of certain specifications and requirements are dependent on specific application considerations. For these, the requirements are provided in terms of a limited number of technology-neutral performance categories, for which it is the responsibility of the authority governing interconnection requirements (AGIR) to consider. Within New England, interconnection requirements vary by state, and further, by Distribution Provider. In New York a common set of DER interconnection requirements exists and there is a Coordinated Electric System Interconnection Request (CESIR) which outlines and initiates the process. Several other State and Provincial AGIR have developed local interconnection requirements which are listed in [Appendix E](#) of this document along with links which will be helpful to access specific interconnection information. These requirements are then supplemented by individual Distribution Provider interconnection agreements, specifications, and requirements.

The DER owner, responsible for its operation, must follow Interconnection Agreements and any AGIR requirements for fault ride-through. Distribution Providers and other AGIR entities should ensure that their requirements describe necessary DER performance with ride-through capabilities for frequency and voltage excursions events. Interconnection Agreements and local requirements generally have provisions to provide documentation upon request.

In addition, NERC developed three NERC Disturbance Reports related to system disturbances in California which resulted in significant inverter-based resource interruptions. The reports may be found on NERC's Major Events Analysis Reports page: <https://www.nerc.com/pa/rrm/ea/Pages/Major-Event-Reports.aspx>. Some of these past events emphasize the importance of fault ride-through.

In terms of generation resource adequacy and resource management there is also the possibility of over generation, as has been demonstrated in the state of California when the system operator runs out of load to absorb the available generation. Operating procedures for selecting which generation to curtail should be in place requiring System Operator visibility of DER either individually or in aggregate. In lieu of operating procedures, some areas of the country are planning to use market mechanisms to address this issue. Interconnection agreements or other state or local requirements may require DER installations to provide communication channels so that generation can be coordinated with a central dispatch authority.

The DER owner's protection and control equipment also should be capable of ceasing to inject current, or automatically disconnecting the generation from the system to which it is directly connected upon detection of frequency or voltage excursion conditions outside of the applicable ride-through requirements. Note that those interconnection agreements, specifications, and requirements should account for both distribution protection and the reliability of the BPS. For three-phase installations, the over and under voltage function should be implemented on each phase and the over and under frequency protection on at least one phase. All phases of a generator or inverter interface should

disconnect or cease to inject current for appropriate voltage or frequency excursion conditions sensed by the protective devices. Voltage protection should be wired as specified by IEEE 1547-2018. Automatic disconnect devices must be sized to meet all applicable local, state, and federal codes.

The specified size of the generation facility or energy storage system should be based on electrical generator or inverter AC nameplate ratings. The specific design of the protection, control, and grounding schemes will depend on the size and characteristics of the DER owner's generation, as well as the DER owner's expected load level. Dynamic protection systems may be needed based on the characteristics of the particular portion of the utility's system where the DER owner is interconnecting.

The settings referenced herein are generally intended for single-phase and three-phase applications using wye grounded- wye grounded service transformers or wye grounded-wye grounded isolation transformers. For applications using other transformer connections, a site-specific review should be performed by the utility and the revised settings identified in the DER Application Process⁷.

The guidance set forth in this document is intended to be consistent with those specifications contained in the most current version of IEEE Std. 1547-2018. It is recommended that the requirements in IEEE 1547-2018 be referenced in the interconnecting utility requirements as well as any further state interconnection requirements as appropriate.

Voltage Response

Within IEEE-1547-2018 and in NY State Public Service Commission Interconnection Requirements, the operating range for the generators is generally intended to be from 0.88 to 1.10 per unit of nominal voltage magnitude. In addition, the generator should not cause the system voltage, at the Point of Common Coupling (PCC), to deviate from a range of 0.95 to 1.05 per unit of the utility system voltage. For excursions outside these limits with a duration longer than the applicable fault ride-through requirements, the protective device generally automatically initiates a disconnect sequence from the utility system as detailed in the most current version of IEEE Std. 1547-2018. Planning Coordinators and Transmission Planners should also be aware that DER installed with older interconnection agreements may reference prior versions of IEEE Std. 1547 and may not meet current ride through requirements. Clearing time is defined as the time the range is initially exceeded until the DER owner's equipment ceases to energize the PCC and includes detection and intentional time delay. Other static or dynamic voltage functions may be permitted or required as agreed upon by the utility and DER owner. The industry is now in the process of promoting ride-through via several different standards initiatives which NPCC is tracking through its DER Forum.

As described above, ensuring that DER can respond appropriately for various voltage conditions is critical for system reliability, as well as avoiding equipment damage and protecting personnel safety. Continuous operation over a wide range of voltage levels will ensure that DER do not prematurely trip or cease to inject current and further deteriorate system conditions. IEEE Std. 1547-2018 includes ranges of

⁷ Currently there has not been an assessment of potential change in sensitivity (increase or decrease) to the effects of Geomagnetic Disturbance (GMD) from the presence of high DER penetration. This is a potential reliability risk to be aware of and evaluated in the future.

trip settings. For inverter-based DER, the “shall trip under” voltage setting should be chosen to meet the requirements of NERC PRC-024-2, as described in Annex B of IEEE Std.1547-2018.

Quebec Interconnection

Ride-through during system disturbances is of primary importance for resources connected to the grid, with the objective of maintaining system reliability⁸. IEEE-1547-2018 addresses the topic, however, for voltage and frequency, what is required in the IEEE standard does not match the requirements in Quebec.

DER should have voltage related operational capability and protection settings set as prescribed by the area Electric Power System (EPS)operator and in accordance with IEEE Std. 1547-2018.

This subject area is a matter of facility installation and personnel policy of the asset owner, balancing both reliability and safety. This information should be communicated to the interconnecting utility for proper protection system coordination.

In the Quebec interconnection voltage ranges and regulation requirements vary from the Eastern Interconnection. The requirements of the AGIR having jurisdiction should be followed (typically the Régie de l'énergie and Hydro-Québec). Details for Quebec’s process may be found in [Appendix E](#).

Frequency Support

Frequency support is provided through the combined interactions of synchronous inertia and frequency response. Working in a coordinated way, these characteristics and services arrest the decline in frequency after a disturbance and eventually return the frequency to the desired level. As increased levels of DER are introduced to the system, synchronous inertia will be displaced, which may have an impact on the frequency response performance of the system. With increased penetration of DER it is becoming desirable for DER to remain connected even outside the prescribed frequency range if there is no risk to the DER equipment. The ride-through curves are “shall not trip within the acceptable range,” not “must trip immediately outside of the acceptable range.”

Interconnection Agreements should require DER to have a frequency and voltage operating range that is equivalent to BPS connected resources consistent with the most limiting of PRC-006-NPCC, PRC-024 and the latest version of IEEE 1547 (IEEE 1547-2018 as amended by IEEE 1547a-2020). The sequence for a protective device to automatically initiate a disconnect sequence from the utility system is also detailed in the IEEE-1547-2018. Clearing time is defined as the time the range is initially exceeded until the DER owner’s equipment ceases to energize the point of common coupling (PCC) and includes detection and intentional time delay. Other static or dynamic frequency functionality may be permitted or required as agreed upon by the utility and DER owner. There should be a mechanism to ensure that the Distribution Provider transmits any necessary information pertaining to capacity, operational characteristics, etc. to system planners and system operators for DER facilities.

Note that in the Quebec Interconnection the frequency operating range is wider than in the Eastern Interconnection. In Quebec, the acceptable steady-state frequency range is from 59.4 Hz to 60.6 Hz, and

⁸ NERC report on Loss of Wind Turbines During System Disturbances : [NERC Report-Loss of Wind Turbines](#)

DER must be capable of riding through frequency as low as 55.5 Hz (for a short time period). Therefore, in Quebec, UFLS systems must operate outside this operating range in accordance with the Quebec variance to the PRC-006-NPCC UFLS-1 regional standard table 4.

Reconnection to the Utility System

If the DER is disconnected as a result of the operation of a protective device, the DER owner's equipment should remain disconnected until the utility's service voltage and frequency have recovered to acceptable voltage and frequency limits for an acceptable amount of time. Interconnection Agreements or local standards should address times for reconnection to the utility system. Per IEEE 1547-2018 Clause 4.10.3, the allowable range of settings is 0-600 seconds with a default setting of 300 seconds. IEEE 1547-2003 in clause 4.2.6 allows an adjustable delay or a fixed delay of 5 minutes. The time specified by the interconnection agreement should be coordinated to support BPS reliability as well as distribution requirements.

DER systems greater than 25 kW that do not utilize inverter-based interface equipment should not have automatic recloser capability unless otherwise approved by the utility. If the interconnecting utility determines that a facility must receive permission to reconnect, then any automatic reclosing functions must be disabled and verified to be disabled during verification testing.

Utilities in other parts of the Eastern Interconnection who have experienced increased levels of DER have determined that during system restoration, DER should not be allowed to return to service until the system has been reestablished and is in a stable operating state. Interconnection Agreements and standards should address necessary communications and SCADA requirements. As traditional resources on the BPS are retired and the grid becomes increasingly reliant on grid edge DER on the Distribution system, Black Start, and System Restoration plans will have to be adjusted accordingly.

Inverters

A power inverter, or inverter, is a power electronic device or circuitry that converts direct current (DC) to alternating current (AC). The inverter itself does not produce power. The power is provided by the DC source. Inverter design and/or configuration should be capable of ride-through for specified utility system events and are grouped into three separate performance Categories.

- Category I is based on minimal BPS reliability needs and is reasonably attainable by all DER technologies that are in common usage today.
- Category II covers minimum BPS reliability needs, and coordinates with NERC Reliability Standard PRC-024-2, which was developed to avoid adverse tripping of BPS generators during system disturbances.
- Category III provides the longest duration and widest range (band) for voltage ride-through capabilities that are attainable by inverter-based systems where very high levels of DER penetration are expected or where momentary cessation requirements are seen as a desirable solution for coordinating with distribution system protection and safety. This category is intended to address DER integration issues like power quality and system overloads caused by DER tripping in the local Area Electric Power System and to provide increased BPS reliability by further reducing the potential loss of DER during bulk system events.

Power Conversion	Prime Mover / Energy Source	Category
Inverter	Solar PV, Battery Energy Storage	Category III ¹ (amended)
	Wind	Category II
	Hydrogen Fuel Cell	Mutual Agreement
Synchronous generator	Bio-/landfill gas, fossil fuel, hydro, combined heat & power	Category I
Induction generator	Hydro	Mutual Agreement
¹ was Category II prior to Amendment		

Figure 2: Example assignment of IEEE 1547 abnormal performance categories to various types of DERs.
Source: Provided courtesy of EPRI⁹

Inverters intended to provide local grid support during system events that result in voltage and/or frequency excursions as described in this document should be provided with the required functionality to allow for the equipment to remain online for the duration of the event.

It is recommended that all applicable inverter-based applications should:

- be certified per the requirements of UL 1741 SA as a grid support utility interactive inverter
- have the voltage and frequency trip settings as specified by the interconnecting utility
- have the abnormal performance capabilities (ride-through)
- provide interactive inverter functions status

In New York State it is recommended that equipment be selected from the Department of Public Service “Certified Interconnection Equipment list” maintained on the NY Public Service Commission’s website. Interconnected DG systems utilizing equipment not found in such list should meet all functional requirements of the current version of IEEE Std. 1547-2018 and be protected by utility grade relays (as defined in these requirements) using settings approved by the utility and verified in the field. The field verification test in New York State must demonstrate that the equipment meets the voltage and frequency requirements detailed in this section. Individual New England State interconnection

⁹ EPRI makes no warranty or representations, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in the Material. Additionally, EPRI assumes no liability with respect to the use of, or for damages resulting from the use of the Material.

standards and agreements also typically refer to IEEE Std. 1547-2018 functional requirements and include protection setting review requirements.

ISO-New England also has developed a technical bulletin, contained in [Appendix F](#), which outlines required settings for inverters in New England.

Certification per UL 1741 SA and UL 1741 SB as grid support utility interactive inverters

Because Inverters currently certified for IEEE 1547-2003 do not currently provide adequate grid support functionality, in the interim period until DER that have been certified as meeting IEEE Std. 1547-2018 in accordance with IEEE Std. 1547.1-2020 (IEEE Standard Conformance Test Procedures for Equipment Interconnecting Distributed Energy Resources with Electric Power Systems and Associated Interfaces) and UL 1741 SB (September, 2020) become available, certification of all inverter-based applications is needed. For example, in one NPCC Area the following approach was taken to assure having inverters installed with a standardized set of grid support functionality to ensure the reliability of the BPS (e.g. maintaining acceptable system frequency and voltage).:

- Should be compliant with only those parts of Clause 6 (Response to Area EPS abnormal conditions) of IEEE Std. 1547.1-2018 (2nd ed.) that can be certified per the type test requirements of UL 1741 SA (September 2016).
- May be sufficiently achieved by certifying inverters as grid support utility interactive inverters per the requirements of UL 1741 SA (September 2016) with either CA Rule 21 or Hawaiian Rule 14H as the Source Requirement Document (SRD). Such inverters are deemed capable of meeting the requirements of this document.
- Applications should have the voltage and frequency trip points and abnormal performance capabilities consistent with IEEE 1547-2018, PRC-024-2 and PRC-006-NPCC “Automatic Underfrequency Load Shedding.”
- For abnormal performance, Category III inverters should be recommended for use. (There may be some circumstances, such as certain types of fuel cells) where the primary energy source may not allow practical implementation of Category III performance. Specification of Category II performance in abnormal conditions may be acceptable in these limited cases.)

UL Standard 1741 Supplement B (UL 1741 SB) implements the test requirements for compliance with IEEE 1547-2018 DER performance requirements in accordance with the test specifications of IEEE 1547.1-2020. With the approval of this UL standard in September 2020, it is anticipated that inverters compliant with IEEE 1547-2018 grid support requirements will be widely available by 2022. Substantial availability of compliant inverters can be anticipated somewhat prior to that date as inverter manufacturers complete their design modifications and move their products through the UL certification process. Once UL 1741 SB inverters become pervasive, the measures in the first and second bullets above are no longer applicable or necessary.

Protective Functions

Protective system requirements for distributed generation facilities result from an assessment of many factors, including but not limited to:

- Type and size of the DER facility
- Voltage level of the interconnection
- Location of the DER facility on the distribution circuit
- Distribution transformer
- Distribution system configuration
- Available fault current
- Load that can remain connected to the DER facility under isolated conditions
- Amount of existing DER on the local distribution system.

Local Interconnection Agreements and standards should require that synchronous, induction and inverter based DER include protection functions for Under/Over Voltage (27/59), Over/Under Frequency (81O/81U), Overcurrent (50P/50G/51P/51G) and Anti-Islanding Protection. Reverse power protection should also be considered as appropriate for BPS support. Interconnection Agreements and standards should require that inverter based DER should be certified according to UL 1741SA as grid supportive. DER protection equipment should utilize a non-volatile memory design such that a loss of internal or external control power, including batteries, will not cause a loss of interconnection protection functions or loss of protection set points. Interconnection Agreements and standards should require that DER protective devices utilize their own current transformers and potential transformers for protection and not share electrical equipment associated with utility revenue metering.

The need for additional protective functions will be determined by the utility on a case- by-case basis. If the utility determines a need for additional functions, it will notify the DER owner of the requirements. The notice should include a description of the specific aspects of the utility system that necessitate the addition, and ideally, explicit justification for the necessity of the enhanced capability. The connecting utility should specify and provide settings for those functions that the utility designates as being required to satisfy their individual protection practices. Any protective equipment or setting specified by the utility is not to be changed or modified at any time by the DER owner without consent from the utility.

The DER owner is responsible for ongoing compliance with all applicable local, state, and federal codes and standardized interconnection requirements as they pertain to the interconnection of DER.

All interface protection and control equipment should operate as specified by state and local interconnection agreements and standards.

In New England, for monitoring and control of new DG projects, [Appendix E](#) lists current interconnection documentation and standards for DER by State. The DER communications hardware, protocols, and data models must comply with these state and local interconnection utility standards.

In New York, for monitoring and control of new DER projects, the most current version of the Monitoring and Control Criteria should be employed by the utilities to evaluate the need for such

equipment in New York. The New York Monitoring and Control Criteria document was developed and agreed to through a collaborative process as part of the Interconnection Technical Working Group (ITWG)¹⁰. The communications hardware, protocols, and data models must comply with local interconnection utility standards.

Also, and fundamentally, existing over-current protections in distribution system are typically designed to clear line and ground faults occurring downstream from their location, as the only source feeding the fault is the transformer station. Connecting a DER provides another source supplying the fault, and the fault contribution from the facility might cause protection to operate non-selectively for reverse faults, out of the protected zone. If the maximum reverse fault current through a non-directional fault-interrupting device exceeds the setting of the device, the fault-interrupting device should be considered with a directional feature to prevent tripping for reverse fault current flow. For instance, phase protection could be replaced with an impedance relay (function 21) if required.

Metering

Advantages and Opportunities of Implementing Advanced Metering Infrastructure (AMI):

IEEE 1547-2018 interoperability requirements specify that the DER have communication capabilities and shall measure specific quantities and have this information available at the communications interface. Most utilities, however, do not have and are not requiring DER owners to provide the communications needed to connect all DER to a grid SCADA system. Such requirements tend to be placed only on large DER. Most utilities do not have the information infrastructure necessary to interoperate with large numbers of small DER; however, implementation of AMI will help in this regard.

Depending on the level of analytics utilized by an Electric Distribution Company (EDC), AMI can provide varying levels of intelligence and operability about the electric distribution system. Even if no analytics are implemented, value can be gained by reviewing and having access to the data provided by AMI. If a full-fledged data analytics package is implemented, then significant benefits can be realized.

Without an analytics package, engineers or analysts can still review basic voltage information provided from AMI. Using SAS, Excel or other simple tools, the voltage data provided, on a daily basis, can be quickly filtered down to exhibit meters that have high or low voltages exceeding the limits set by local Regulatory bodies. With minimal research, it can be determined if high voltage is caused by the presence of DER, either for the meter affected or a nearby neighbor on the same secondary transformer. The transformer can be evaluated by engineering to determine if new, larger equipment is needed.

With reports of abnormal voltage, Distribution Planning can evaluate the data and determine if voltage regulators need to be added towards the end of a circuit, if switching needs to occur to change circuit topology, or if other actions are needed. If the low voltage only occurs at certain times of the day, then perhaps load tap changers at the substation may be used to address the issue.

¹⁰ This document can be found on the Department of Public Service website (www.dps.ny.gov) at the Distributed Generation/Interconnections tab under Interconnection Technical Working Group Information.

If implementing a data analytics package, whether off-the-shelf or home grown, more details on system operating conditions can be found. For instance, by evaluating the sum of meter usage for a specific transformer, secondary transformers can be determined to be over or under loaded. If voltage interval data is available, the GIS model of the system can be evaluated to identify meters that are incorrectly assigned to transformers; the model can be corrected to properly assign meters to transformers.

With data analytics and near real-time data transfer from the head-end system then volt-var optimization can occur. As LTCs, capacitor banks or voltage regulators are adjusted, live feedback from the system can be evaluated to ensure the expected responses are occurring. If something unexpected is happening, then operators receive evidence of this quickly and can take remedial actions.

The specific benefits of AMI are still evolving, and as more analytical tools are made available, and as meters become more advanced, the data will be leveraged to provide more insights into the operation of the distribution network.

Metering requirements for SCADA purposes are usually determined by the local connecting utility and based on the configuration of the DER system prior to energization. Whether SCADA metering can be integrated with revenue metering is a matter for the local connecting utility and connecting DER facility to decide. New metering or modifications to existing metering should be reviewed on a case-by-case basis and be consistent with metering requirements specified by the local connecting utility and any overarching requirements adopted by the local regulatory authority that has jurisdiction (e.g. state commission for example for revenue metering).

IEEE-1547-2018 requires DER to be capable of providing monitoring of connection status, real power output, reactive power output, and voltage either at the point of connection or some agreed upon point if multiple DER facilities are involved. Going forward, member utilities should consider developing IT Infrastructure plans to aggregate and report critical DER Status to BPS Operators, i.e. aggregate DER output within a given area and map those to individual transmission nodes. This information should be available to the system operator as required by the connecting utility. The monitoring equipment should be installed at the time of interconnection and meet the technical requirements of the connecting utility. The DER metering and monitoring communications will allow interoperability and the capability to provide system operators with situational awareness necessary for reliable operation of the interconnecting utility facilities. As more DER is employed and base load generation is replaced with DER resources, it will be important for the Distribution Provider (DP) or interconnecting utility to be able to monitor the availability and production of electricity (power output and energy delivered) from the DER resources.

Power Quality

In practice, DER-related power quality issues are exclusively distribution issues and have little impact or relevance to the bulk power system, or to power quality in other distribution systems. Therefore, this topic is not addressed in this document.

Power Factor

IEEE 1547-2018 requires new DER to have the capability to produce or absorb reactive power from 0.95 pf leading to 0.95 pf lagging¹¹. The standard also specifies that DER have a number of different control functions to regulate this reactive power capability. Legacy DER are typically operated at unity power factor.

Because of the low reactance to resistance (X/R) ratio of distribution systems, the general impact of DER active (kW) power at high penetration is to elevate distribution voltages, potentially to excessive levels. Utilization of DER reactive power capabilities will generally mean that these DER will be absorbing reactive power during high output in order to hold down the distribution voltage to acceptable levels.

Transmission system voltage are generally decoupled from distribution system voltage levels by on-load tap changers in primary distribution substation transformers. The increased reactive power demand that can be brought about by deployment of DER reactive power to mitigate distribution overvoltage issues, however, can directly impact the transmission system unless that additional reactive power demand is compensated by capacitor banks at the distribution substation bus. This can increase total reactive power demands on the transmission system and could potentially have adverse impacts on bulk system voltage stability.

Islanding

Although an entire distribution substation along with some transmission assets could become islanded in a very high DER penetration scenario, islanding is primarily a distribution system concern. IEEE Std 1547.1-2020 tests certified DER for islanding detection with the most insensitive trip settings and with the most aggressive grid support functions. Because DER must pass the islanding detection tests despite these settings and functions, islanding concerns should not be a constraint on implementing trip settings and disturbance ride-through requirements that are necessary for protecting the bulk system security from the impacts of widespread DER resource tripping due to transmission level disturbances.

Some of the anti-islanding algorithms that are implemented in DER intentionally destabilize islanded systems in order to force voltage or frequency tripping. There is some concern that, at high regional DER penetration, these functions may also have adverse impact on the dynamic stability of the bulk system. This potential issue is in need of research to define its extent and severity.

Automatic Underfrequency Load Shedding (UFLS) Programs

UFLS is implemented to restore power system frequency stability if system frequency drops below the UFLS operational set point. Significant deviations in system frequency typically occur during major disturbances such as a loss of generation or events in excess of design contingencies used for planning purposes. UFLS is considered the “safety net” for the BPS and a last resort automatic operation designed to stabilize BPS islands for a generation deficiency. Various fractions of load are shed in multiple stages, up to about 31% of peak net load¹², in order to stabilize frequency. UFLS is primarily installed on distribution feeders, where DER is increasingly being deployed.

¹¹ Certain DER, such as rotating generators, may be allowed to meet slightly less stringent reactive power requirements.

¹² Peak net load shall be calculated as an average of the peak net load from the previous 3 years, excluding the

NERC has a set of requirements in the PRC-006 standard and NPCC has more stringent requirements in NPCC's Regional Standard, PRC-006-NPCC¹³ which outline expected UFLS performance. Approved and effective versions of these standards may both be found on the NERC website.

SS-38 is the NPCC working group responsible for inter-Area dynamic analysis. The SS-38 Working Group regularly studies the UFLS performance within the Region and has recently completed sensitivity analysis showing that a moderate increase of DER penetration anticipated in the short term will not result in any significant degradation in the UFLS program performance based on the conditions and assumptions used in the analysis.

In the future, adopting a more flexible approach to UFLS may be necessary as DER penetrations reach higher levels. There are utilities that are reviewing the feasibility of "Adaptive UFLS" which uses real time monitoring of distribution feeder loads and their DER to determine how much additional load may need to be tripped when DER has increased output. Some utilities, such as Duke Energy avoid choosing those distribution feeders for the UFLS program that have DER interconnected to them.

Effective Grounding for DER

The subject of Effective Grounding may not, in many cases, be impactful to BES reliability it will potentially have an impact on Substation equipment, particularly substation class metal oxide varistor (MOV) arrestors due to overvoltages during faults. With the onset of high penetrations of DER, such as photovoltaic (PV) generation, utilities should consider interconnection of DER similarly to how they would interconnect synchronous generators.

Conventional generators are considered voltage sources as the magnetic flux within the generator tends to provide a constant voltage source during faults. In contrast, inverter-based DER are considered voltage-controlled current sources during faults. Inverter-based facilities generally provide less short-circuit current than similarly sized synchronous units.

Solidly grounding a transformer neutral for a DER plant eliminates a possible phase overvoltage stemming from a single-line-to-ground fault. A potential problem with the solid grounding in the distribution line is that large fault currents can flow through the transformer neutral, which can desensitize the overcurrent protection coordination. In order to mitigate this issue, impedance grounding can limit the fault current and potential equipment damage, while allowing overvoltage to some limited magnitude. Some utilities protect their distribution from overvoltage by using overvoltage protection so Effective Grounding isn't a concern. Further investigation on the how specific installations are grounded is warranted and being pursued by the Interconnection Technical Working Group (ITWG) in New York.

current year. See NPCC's Regional Standard for further details on UFLS requirements, PRC-006-NPCC-2 [Automatic Underfrequency Load Shedding](#)

¹³ Effective Date of the Standard is 4/1/2020 subject to the Implementation Plan and specific area regulatory approvals

Resource Adequacy

Forecasting resource adequacy is an important system reliability planning function¹⁴. The reporting of generation capability and related performance data is integral to this activity. Specific modelling information of intermittent DER resources is critical to planning and understanding system performance. Information related to DER in-service dates, capacity value, availability, emergency assistance, scheduling, and deliverability should be available to the planners. Modeling, data, and other necessary information should be defined and made available to those needing it, such as system planners and system operators. Any requirements associated with this information should be in Interconnection Agreements or Tariffs prior to any commissioning of the DER. Mechanisms for DER entities to provide this information are evolving, depending on locality, and subject to change as DER penetration increases.

Energy Storage Systems for DER

Battery storage technology is undergoing a rapid evolution from Lead Acid to Absorbent Glass Mat to Li-Ion due to the expanding application of batteries to transportation and other sectors. Li-Ion batteries have been and continue to be deployed in a wide range of electric energy-storage applications, ranging from energy-type batteries of a few kilowatt-hours in residential systems with rooftop photovoltaic arrays to multi-megawatt containerized batteries for the provision of grid ancillary services. The Energy Storage Association (ESA) anticipates at least 35 GW of new energy storage will be deployed in the United States by 2025.

NPCC is also observing marked increases in Hybrid Resources which are combinations of multiple technologies that are physically and electronically controlled by the Hybrid Owner/Operator behind the point of interconnection (“POI”) and offered to the grid as a single resource at that POI. This arrangement usually involves energy storage at a photo-voltaic or wind turbine site. It optimizes the use of DER and enables normally clipped energy (energy beyond the rating of an inverter or unneeded by the BPS) to be stored on-site and released in the future. It also allows low outputs of DER which may be outside the operational range of an inverter to be harvested for charging on-site storage allowing better utilization of the total resource. In the figure below the red curve represents the capability of an inverter and the blue is the capability of the DER. Areas between the curves may be used to charge or be “harvested.” This leads to a more efficient utilization of the DER and supports grid reliability and state of charge of the energy storage. As shown in Figure 3 below, the capability of an inverter can be exceeded by the capability of the DER behind it. Figure 3 below also displays a typical daily capability curve associated with a PV inverter with the maximum power capability delivered during mid-day. DER in many instances is designed with due consideration of the degradation of capability, such as a solar panel’s capacity over time.

¹⁴ For background on resource adequacy metrics see: [“Resource Adequacy Metrics and their Applications”](#) prepared by the New York State Reliability Council.

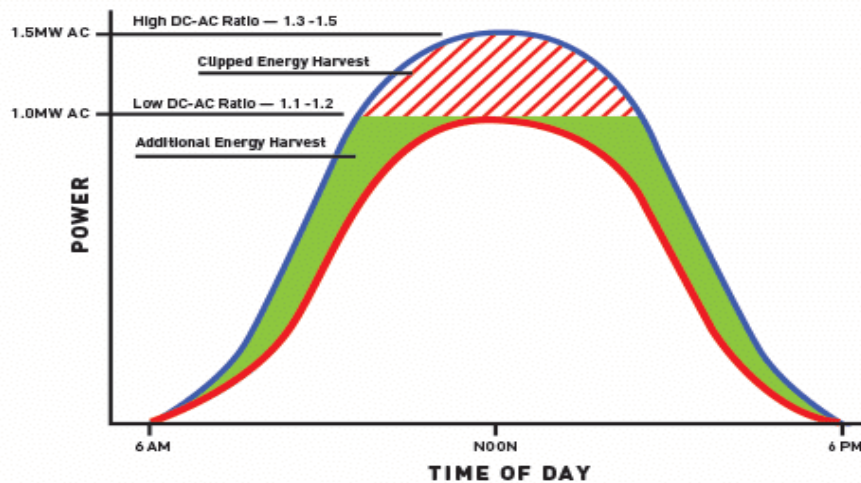


Figure 3- Storage showing Clipped and Unused Energy

The ESA has an online report to manage any risks associated with Energy Storage. Their report may be found here, [Energy Storage, Operational Risk Management](#). Care should be used in placement of batteries and should avoid physical proximity (due to the risk of fire or explosion) and electrical proximity (due to harmonics and other power electronic interaction concerns) to other facilities that may be critical to the reliable operation of the BPS.

System Control and Data Acquisition (SCADA) and Communications

As DER penetration increases all DER above a certain MW level, as determined by the interconnecting utility or System Operators, should be required to provide SCADA telemetry data to a control center to monitor their output. It might be beneficial to have DER data be communicated to a Distribution System Operator, distribution system platform or similar, to provide analysis and aggregation of data for a concise summary to the transmission system operator. IEEE-1547-2018 has a communication port requirement. This ensures that the output remains visible to the system operator. It allows the system operator to observe DER status when working on a feeder in emergency or planned outage situations. Some NPCC Members have encountered difficulty with obtaining information and data from DER operators. DER owners should be encouraged to keep their end of any SCADA equipment functional and reconnect their telemetry devices when they have been disabled and this can be done through interconnection requirements. The operator should be alerted by the DER when telemetry is interrupted. Scan rates equivalent to the scan rates used by the system operator are preferred (typically in the 6 second range). Although IEEE 1547-2018 defines and requires a communication port, the path that a utility may use for data from that communication port may pose a cyber-security risk if not adequately secure. It is suggested that full consideration be given to cyber security risks when transferring data until such time as the IEEE 1547 has been amended to require cyber security protections.

Going forward many areas and utilities are either in the process of or determining the value of adding distribution system platforms to deal with DER aggregation, observability, availability and status of DER. NPCC will continue to monitor the development and deployment of these Distributed Energy Resource Monitoring Systems (“DERMS”).

DER Recommendations

As DER continues to proliferate within the NPCC Region we suggest the following initial activities:

Participation in National DER Forums

- 1) Participate in efforts to fully understand the issues and best practices associated with DER.
- 2) Engage NPCC and its members to address the issues and provide expertise.
- 3) As the understanding of the issues and best practices matures, then NPCC will be well positioned to understand the regional differences that need to be considered.

Process and Risk Management Recommendations

- 1) Continue with sensitivity analysis at the Transmission level for various levels of penetration of DER on the distribution facilities to determine effects of increased penetration levels of DER on BPS performance.
- 2) Pursue further opportunities to coordinate distribution and transmission requirements for DER, share Member best practices, and promote consistency regarding DER installations where possible within the NPCC region.
- 3) Continue to review and identify approaches to coordinate NPCC AGIR and utility interconnection requirements relative to DER to identify dissimilarities between Areas which may negatively impact reliability.
- 4) Identify opportunities to share information regarding DER related reliability risk problems and solutions and promote sharing.
- 5) Encourage consideration of developing IT Infrastructure plans to aggregate and report critical DER Status to BPS Operators.
- 6) Continue to solicit and address observable reliability related issues of DER using NPCC's DER Impact Reporting Forms and its associated process.
- 7) Continue to discuss any changes required for System Restoration and Blackstart Plans, as a result of increased DER.
- 8) Continue to follow DER related ESA ESS safety issues and associated recommendations and share the results with NPCC stakeholders.
- 9) Avoid placement of UFLS on distribution feeders which have a significant amount of DER relative to the feeder's load if possible, unless sufficient telemetry exists to ensure proper functionality of the UFLS program as a whole.

Planning Related Recommendations Due to Changing Resource Mix

- 1) Identify and consider new methods to obtain and facilitate collection of DER modeling and performance data to enable Long-Term Resource, Long-Term Transmission and Operational Planning of the BPS¹⁵
- 2) Clearly identify DER in the NPCC Region's Area interconnection queues or forecasts where DER is being proposed for installation, including the magnitude and location relative to the existing resource base and load projections.
- 3) Address masking of load by DER at the distribution level to ascertain its impact on the behavior of load, as well as the assumptions that underpin UFLS programs.
- 4) Determine the appropriate entities responsible for providing DER data to the Planning Coordinator for the purposes of model building and maintenance and ensure that this data is provided.

Analytics and simulation recommendations to deal with increased system complexity

- 1) Support interconnection wide inertia loss study efforts, to determine potential reliability impacts, as DER replaces conventional synchronous generation resources.
- 2) Obtain DER modelling data to be able to model, predict and examine system behavior and assess the interactions between the new resources and the existing reliability preserving systems and programs. Examples include:
 - a. Dynamic behavior of the transmission system
 - b. Sudden loss of large amounts of DER due to transmission system events
 - c. Under Frequency Load Shedding,
 - d. Under Voltage Load Shedding,
 - e. Frequency response sharing mechanisms (BAL standards).
 - f. Analysis of system protection systems (both T and D) so that the parameters to set protection systems and other control systems are known to permit the most reliability benefits to be garnered from the new resources.
- 3) Determine the transmission and distribution benefits and challenges of DER fault-related dynamic voltage support.
- 4) Determine the value to the transmission and distribution systems of the different DER steady-state voltage/reactive power control.

Implementation of IEEE-1547-2018

- 1) Work with the AGIR to assign abnormal performance categories for DER certified as meeting IEEE Std. 1547-2018. For example, synchronous generators could be Category I. All inverter-based generation could be Category III. Exceptions could be allowed for inverter-based technologies that could not meet category III and did not constitute a significant penetration. Exceptions could need to be agreed to by both the distribution and transmission entities.
- 2) Develop standard voltage trip settings (1547-2018 Clause 6.4.1) that provide for BPS reliability. For example for Category III, UV1 could be set at 0.88 p.u. & 3.5 seconds to coordinate with PRC-

¹⁵ Questions exist regarding which entities should be responsible for providing DER data to the Planning Coordinator for the purposes of model building. NERC is working on this issue.

024-2 at 0.88 p.u. & 6 seconds to coordinate with PRC-024-2 with margin for Fault Induced Delayed Voltage Recovery (FIDVR) or at 0.88 p.u. & 10 seconds which conforms with the default setting of Category II I. UV2 could be set at 0.5 p.u. and 2 seconds which conforms with the default setting of Category III.

- 3) Develop standard frequency trip settings (1547-2018 Clause 6.5.1) that provide for BPS reliability. For example, use the default setting which were chosen to coordinate with under frequency load shedding.
- 4) Develop standard frequency droop settings (1547-2018 Clause 6.5.2.7) that provide for BPS reliability. For example, use the default settings that are consist with the requirements for generators connected to the BPS
- 5) Develop standard Enter Service settings (1547-2018 Clause 4.10) that can be used in black start studies. The default delay time is 300 seconds. However, distribution entities may require a shorter delay to reduce the impact of cold load pickup. Also, distribution entities may require different delay times when several large DER are connected to the same feeder
- 6) Develop requirements that ensure protective relay settings on the distribution system coordinate with the voltage and frequency ride-through capabilities established by the selected trip settings. Any exceptions shall be discussed with the transmission provider.

Appendix A, NPCC DER Impact Reporting Form and Process



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Please Complete and email this form and email to; [npccstandard@npcc.org](mailto:npscstandard@npcc.org)

Distributed Energy Resource (DER), BES Impact Reporting Form

Name		Date	
Email		Company	
Impact on Bulk Electric System		Area (NY, NE, State or Province etc.)	

Equipment Impacted

Equipment	Location (substation name, etc.)	Impact (Positive reliability impact? Negative reliability impact-Protection System failure, Misoperation, load affected or lost?, power quality issue?, etc.)	Duration of Impact, (start and stop times, length of impact, ongoing? etc.)

Description of Impact on BES- What Happened or was observed?

Please describe below the details of all the impacts of the DER as it pertains to this report, such as load loss, loss of life, equipment failure or potential reliability improvement. A sequence of events showing the impact is helpful. Attach supporting information to this form if necessary.

Root Cause or additional Analysis

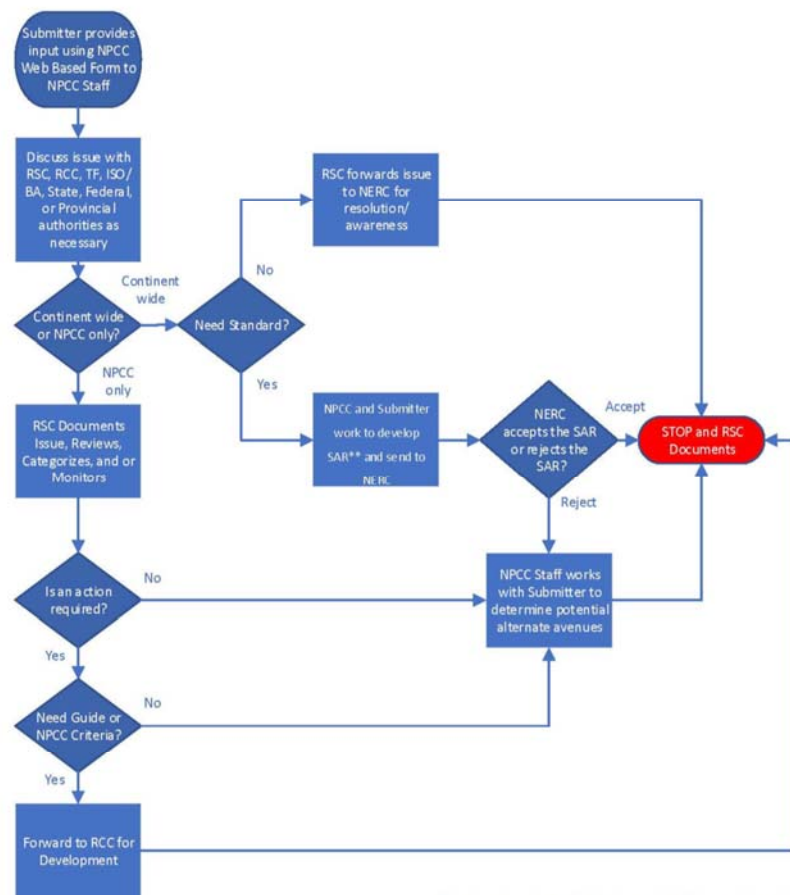
Please describe below the details of any investigation your company may have already done to identify causes or contributing factors to the incident. This will help NPCC route the issue properly to address it.

NPCC Review of Issue and Recommendations (i.e. refer to NERC, develop a Criteria, Guideline, Already Addressed or Identified, etc.)

NPCC Date of Resolution of Issue _____

Evaluation Process

Impacts from Distribution Level* Distributed Energy Resources on the BES



*Distribution Level, Not behind the Meter, utility scale DER

** Standards Authorization Request (SAR)

Regional Standards Committee, Approved 8/22/18 (GVZ)

Appendix B, NPCC Areas- Comparisons

Key Inverter based specification extracts

	ISO-NE Inverter Requirements	NG ESB 756 B, C, D	NY SIR ¹⁶	IESO F2 Technical Requirements
Inverter Certification	yes	yes	yes	yes
Voltage and frequency trip settings for inverter-based applications	yes	yes	yes	yes
Voltage Response	yes ¹⁷	yes	yes	yes
Frequency Response	yes ¹⁸		yes	yes
Abnormal performance capability (ride-through) requirements for inverter-based applications	yes	yes		
Other grid support utility interactive inverter functions statuses	yes			
Minimum protection functions		yes	yes	
Monitoring and Control		yes	yes	yes
Reconnection to the System		yes	yes	
Distribution Protection Coordination		yes		yes
Inverter Certification		yes	yes	
Power Quality			yes	

¹⁶ NY SIR is the [New York Standardized Interconnection Requirement](#).

¹⁷ The functionality is required to be present, but the default state is to have this functionality disabled unless otherwise directed by the area EPS operator

¹⁸ The functionality is required to be present, but the default state is to have this functionality disabled unless otherwise directed by the area EPS operator

Appendix C – SPIDER Working Group Reliability Guidelines & Activities

The NERC System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG) was formed to focus on the impacts that aggregate amounts of DER can have on transmission planning and BPS reliability. This SPIDERWG is seeking to provide high-level, technical recommended practices for ensuring BPS reliability in the face of growing penetrations of DER across North America. The recommended practices and guidance provided by SPIDERWG, in many cases, will need to be adapted to specific utility and regional planning and operating practices. The following DER-related topics are covered, as described in NERC Staff's "Summary of Activities: BPS-Connected Inverter-Based Resources and Distributed Energy Resources"¹⁹:

Modeling: Representing aggregate DER in BPS reliability studies, advancing industry capabilities and expertise with representing DER in these reliability studies, developing robust and reasonable data sets for power flow and dynamic simulations

Verification: Ensuring that the models used in studies provide a reasonable and suitable representation of the actual aggregate performance of these resources, benchmarking software platforms to ensure uniformity in tools, recommending analysis techniques for accounting for aggregate DER during large BPS disturbances

Studies: Improving study techniques and methods to ensure the most stressed operating conditions are chosen for BPS reliability studies, identifying key operating conditions and sensitivities to perform, improving software tools and study capabilities

Coordination: Supporting coordination between transmission and distribution entities for improved data exchange and coordinating with IEEE to support the application of IEEE Std. 1547- 2018 across North America

A list of SPIDERWG Reliability Guidelines and other activities is provided in Table 1 and Table 2, respectively.

¹⁹ Available here: https://www.nerc.com/comm/PC/Documents/Summary_of_Activities_BPS-Connected_IBR_and_DER.pdf

Table 1. SPIDER Working Group Reliability Guidelines

Subgroup	Title	Description	Status
Modeling	DER Data Collection for Modeling	Guideline providing recommended practices for collecting DER data for the purpose of developing aggregate DER models for BPS reliability studies.	In Review – Draft Posted for Comment (here)
	DER_A Model Parameterization	Guideline providing recommendations for using state-of-the-art aggregate DER dynamic models in BPS reliability studies.	Published (here)
Verification	DER Performance and Model Verification	Guideline providing recommended practices for performing model verification for aggregate DER dynamic models including placement of measurement devices, execution of verification simulations, and how to use the data collected through these practices.	In Development
	DER Forecasting Practices and Relationship to DER Modeling for Reliability Studies	Guideline providing how forecasting practices are linked to DER modeling for reliability studies, specifically on how DER are accounted for in future reliability assessments.	In Development
Studies	Bulk Power System Planning under Increasing Penetration of Distributed Energy Resources	Guideline providing recommended practices for performing planning studies considering the impacts of aggregate DER behavior.	In Development
	Recommended Approaches for Developing Underfrequency Load Shedding Programs with Increasing DER Penetration	Guideline regarding how to study UFLS programs and ensure their effectiveness with increasing penetration of DER.	Under Consideration
Coordination	BPS Reliability Perspectives on the Adoption of IEEE 1547-2018	Guideline providing industry recommendations and BPS reliability perspectives on the implementation and adoption of IEEE 1547-2018.	Published (here)
	Communication and Coordination Strategies for Transmission Entities and Distribution Entities regarding Distributed Energy Resources	Guideline recommending strategies to encourage coordination between Transmission and Distribution entities on issues related to DER such as information sharing, performance requirements, DER settings, etc.	In Development

Table 2. SPIDER Working Group Other Activities

Subgroup	Title	Description	Status
Modeling	Modeling Notification: Dispatching DER off Pmax in Case Creation	Notification of accounting for DER in powerflow and dynamics cases, particularly regarding accounting for power output levels with DER utilizing advanced grid-supportive features.	Posted (here)
	DER Modeling Survey	Survey of SPIDERWG member organizations regarding the use of DER models in BPS planning studies.	Compiling Results
Studies	White Paper: Review of TPL-001-5 for Incorporation of DER	White paper discussing technical review of NERC TPL-001-5 in the context of increasing DER and their impacts to the BPS. Possible SAR development following completion of white paper, as needed.	In Review
	White Paper: Recommended Simulation Improvements and Techniques	White Paper recommending simulation software improvements to enhance the ability to accurately account for and model DER.	In Development
	White Paper: DER Impacts to Undervoltage Load Shedding	White Paper briefly discussing how DER may impact UVLS program development.	In Development
	White Paper: Beyond Positive Sequence RMS Simulations for High DER	White Paper highlighting the use of tools that provide additional technical detail to DER studies beyond just positive sequence RMS simulation tools.	In Development
Coordination	Coordination of DER Terminology	Development and ongoing review of definitions and terminology pertaining to DER and related topics.	In Development
	NERC Reliability Standards Review	White Paper reviewing NERC Reliability Standards and the impacts that increasing penetrations DER may have on BPS reliability and standards compliance/implementation. Possible SAR development following completion of white paper, as needed.	In Development
	Tracking and Reporting DER Growth	Coordinated review of information regarding DER growth, including types of DER, size of DER, etc. Consideration for useful tracking techniques for modeling and reliability studies.	In Development

Appendix D, NPCC Reliability Principles

Using its membership structure and governance authority to create and apply Regional Criteria²⁰, NPCC Member adherence to Regional Criteria contributes to a more robust level of reliability beyond NERC ERO reliability “results-based” standards / requirements. For example, NPCC Criteria mandate specific design requirements for NPCC Member facilities. NPCC’s approach to reliability and Resilience can be summarized in Principles that guide NPCC Members in their effort to meet or exceed NERC requirements. NPCC’s core Reliability Principles²¹ and activities support the NERC Bulk Electric System and NPCC’s Bulk Power System reliability.

The NPCC Reliability Principles include:

1. **Focus on the most important system components:** In order to focus resources to those portions of the power delivery system most important (critical) to overall reliability, NPCC Members employ mechanism(s) for identifying those facilities that are most critical to the reliable planning and operation of the power delivery assets in the NPCC region²². These critical facilities collectively are identified as the NPCC Bulk Power System^{23,24}.
2. **Application of Criteria beyond NERC requirements to identified critical facilities:** Where, in the opinion of NPCC’s Membership, the NERC standards do not adequately specify a necessary performance or design outcome in a given technical, operation or planning area, NPCC Criteria govern the design of their respective portions of the NPCC Bulk Power System planning and operation²⁵ activities.
3. **NPCC Members support the Criteria:** NPCC’s Full Members in accordance with the NPCC Bylaws are committed to designing and operating their systems to meet the NPCC Criteria under peer review of the NPCC Full Members.
4. **No conflict with NERC Requirements:** The NPCC Criteria supplement, improve upon where necessary, benefit, and do not conflict with or duplicate the results-based performance

²⁰ See NERC Rule of Procedure #313 on page 15 of the [NERC Rules of Procedure 3-9-2018](#).

²¹ The Reliability Principles were summarized in the NPCC 2018 Strategic Review Report.

²² The method of identifying critical facilities is currently embodied in the [NPCC A-10 Classification of bulk power system Elements](#) document, currently under review by the CP-11 Working Group with a due date of October 31, 2018.

²³ The NPCC bulk power system is identified by a specific list of facilities in the NPCC region deemed critical by the NPCC A-10 classification process. This list is not determined based on the definition of the ERO bulk power system, which is defined in the US 2005 EPACT as:

“(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

“(B) electric energy from generation facilities needed to maintain transmission system reliability.

The term does not include facilities used in the local distribution of electric energy.

²⁴ There are other documents which supplement the Directories, for instance the NPCC Compliance Guidance Statements. These documents usually refer to NERC standards applicability and can be found here: [NPCC CGS](#)

²⁵ NERC [Rule of Procedure](#) #313 (page 15) permits the following: “Regional Entities may develop Regional Criteria that are necessary to implement, to augment, or to comply with NERC Reliability Standards, but which are not Reliability Standards. Regional Criteria may also address issues not within the scope of Reliability Standards, such as resource adequacy. “

requirements of NERC standards where they apply to the NPCC Bulk Power System. NPCC adjusts its Regional Criteria to retire or adapt to any new NERC requirements as they come into effect as necessary.

5. **Include design specifications where needed:** The NPCC Criteria and related guidelines and procedures provide design criteria and practices to assure implementation. NPCC Directories go into greater detail regarding how to accomplish a given reliability result, where NERC standards may simply require a “reliability result.”
6. **Resilience has always been an element of NPCC Criteria:** Based on experience, resilience^{26 27} is a necessary constituent component of reliability and it is important both to electricity consumers and regulatory authorities in NPCC’s Region. NPCC Criteria provide substantial resilience benefits to the NPCC Bulk Power System by providing:
 - a. Robustness – The ability to withstand disturbances by supporting operations in a more secure state.
 - b. Resourcefulness – The ability to detect and manage a crisis as it unfolds.
 - c. Rapid recovery – The ability to get services back as quickly as possible in a coordinated and controlled manner.
 - d. Adaptability – The ability to absorb new lessons from events

²⁶ Reference NERC’s recent [filing](#) with FERC regarding Resilience for a more complete discussion of the relationship between resilience, the NERC standards and the NAICS Resilience Framework. FERC is expected to define resilience in the course of its current examination of electric system resilience concepts.

²⁷In the US, [Presidential Policy Directive – 21](#) defines resilience as “The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents”.

NERC, Model of Resilience

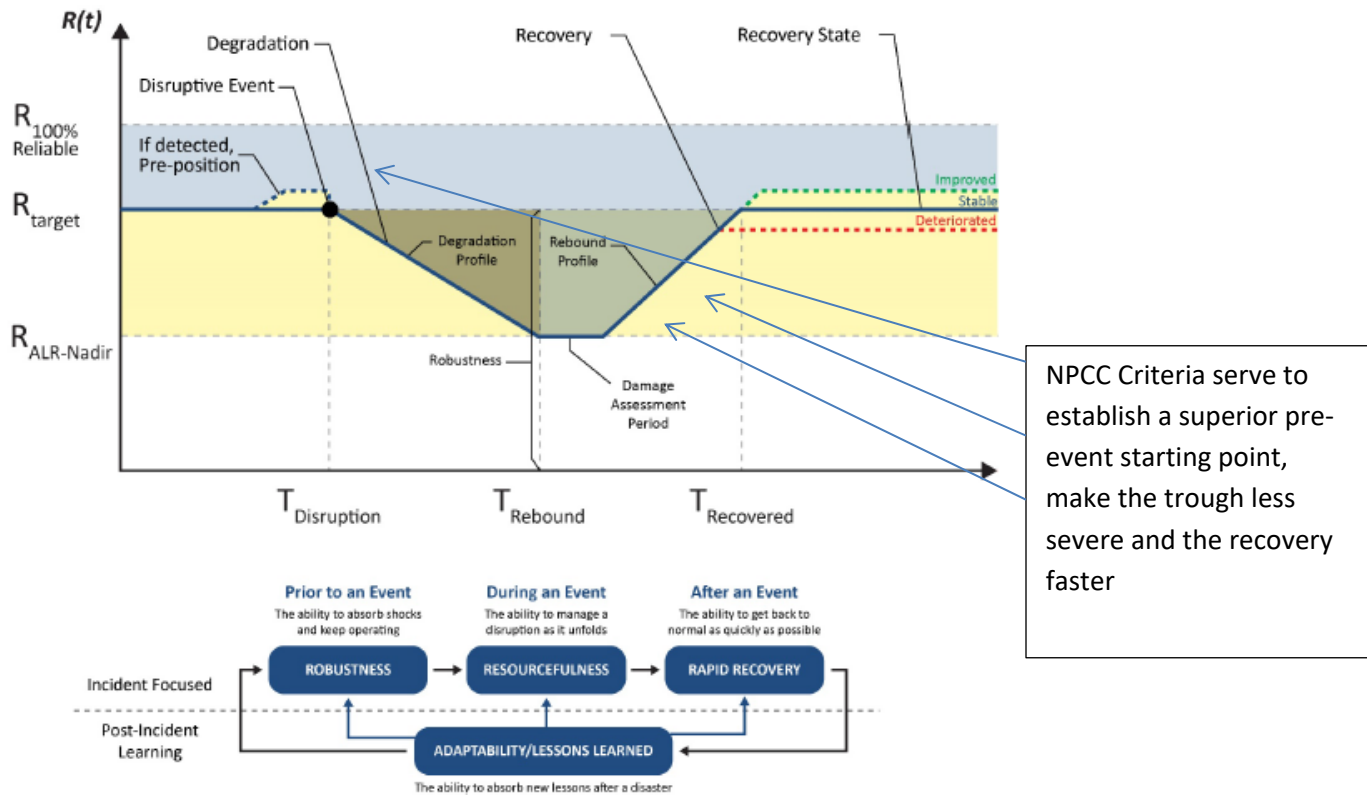


Figure 2.1

Figure 2.1 depicts a typical disruptive event and maps how the systems responds in a qualitative fashion. The y-axis above is meant to represent a relative level of reliability and system response is plotted temporally. DER will increasingly fill a critical role with respect to reliability and Resilience of the Bulk Electric System. Specifically, DER can contribute to the overall robustness of the system and provide increased resource support within islands during system separations. As DER continues to penetrate the system, changes to NPCC's Underfrequency Load Shedding program may be required.

Appendix E, State and Provincial AGIR Information

New York State

Statewide Interconnection Technical Documents may be found at:

[Interconnection Technical Working Group Webpage](#)

New England, by State

Inverter Source Requirement Document of ISO New England (ISO-NE)

Connecticut –

Department of Energy and Environmental Protection, Public Utilities Regulatory Authority (PURA)

Eversource Energy – Connecticut Interconnection Standard

<https://www.eversource.com/content/general/about/about-us/doing-business-with-us/builders-contractors/interconnections/connecticut-application-to-connect>

Summary of Facility Connection Requirements for Generation, Transmission and End Users Connecting to UI Transmission Facilities, Revision 4.0, December 7, 2015:

<https://www.uinet.com/wps/wcm/connect/89138d72-c4a0-403b-9871-937a00f91c42/NERC%2BFAC-001%2BInterconnect%2Bsummary%2BDocument%2BRevision%2B4.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-89138d72-c4a0-403b-9871-937a00f91c42-mkr0qCb>

Eversource/United Illuminating Guidelines for Generator Interconnection, Fast Track and Study Processes, April 5, 2019:

https://www.uinet.com/wps/wcm/connect/bd802aec-1e83-4051-8a6e-58f0cb98d1fd/Guideline_for_Generator_Interconnection_Fast_Track_and_Study_Process_5-12-10_doc_1577.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-bd802aec-1e83-4051-8a6e-58f0cb98d1fd-miUZQ4n

Maine –

Maine Public Utilities Commission

Chapter 324 Small Generator Interconnection Procedures

Central Maine Power Transmission and Distribution Interconnection Requirements for Generation, December 15, 2018:

<https://www.cmpco.com/wps/wcm/connect/dee5fbf1-7af0-40ec-b06c-af3ec015e0be/SchB-TransmissionDistributionInterconnectionRequirementsforGeneration.pdf?MOD=AJPERE&CACHEID=ROOTWORKSPACE-dee5fbf1-7af0-40ec-b06c-af3ec015e0be-mwfmMCK>

Emera Maine Interconnection Agreement:

<https://www.emeramaine.com/energy-solutions/connecting-renewable-resources/small-generator-interconnection-process/>

Massachusetts –

MA Department of Public Utilities (MADPU) interim guidance (DPU 19-55)

MADPU Massachusetts Department of Energy Resources

MADPU Interconnecting Renewable Energy webpages with links to: resources, past and present proceedings before the DPU, each electric distribution companies' tariff, and the Ombudsperson dispute resolution process: <https://www.mass.gov/interconnecting-renewable-energy-facilities>

MADPU is currently conducting a large-scale investigation into the rules and procedures by which distributed generation is interconnected in Massachusetts in docket D.P.U. 19-55. This investigation includes implementation of IEEE 1547-2018. Documents and information can be found in our online file room: <https://eeaonline.eea.state.ma.us/DPU/Fileroom/dockets/bynumber> (enter "19-55")

Massachusetts Technical Standards Review Group:
<https://sites.google.com/site/massdgic/home/interconnection/technical-standards-review-group>

Renewable energy generally: <https://www.mass.gov/topics/renewable-energy>

MADPU Net Metering Information: <https://www.mass.gov/net-metering>

MADOER SMART Program Information: <https://www.mass.gov/info-details/solar-massachusetts-renewable-target-smart-program>

Who to contact in MA for your renewable energy question: <https://www.mass.gov/info-details/who-to-contact-about-my-renewable-energy-question-or-concern>

Massachusetts Utilities

National Grid / Supplement to Specifications for Electrical Installations / ESB 756-2019 ver. 5.0 (Section 7.8 includes voltage and frequency ride through and control requirements);

https://www9.nationalgridus.com/non_html/shared_constr_esb756.pdf

NSTAR ELECTRIC COMPANY d/b/a EVERSOURCE ENERGY STANDARDS FOR INTERCONNECTION OF DISTRIBUTED GENERATION, M.D.P.U. No. 55, Effective: February 1, 2018:

https://author.eversource.com/content/docs/default-source/rates-tariffs/ma-electric/55-tariff-ma.pdf?sfvrsn=8582c462_6

Unitil Energy Systems, Inc. Interconnection Standards for Inverters Sized up to 100 kVA:

https://unitil.com/sites/default/files/pdfs/UES%20100%20KVA%20Interconnect%20Standard%202009_08_21_1.pdf

Individual Massachusetts Municipal Electric Utility Entity Interconnection Requirements:

<https://www.mass.gov/guides/net-metering-guide>

New Hampshire –

New Hampshire Public Utilities Commission

Liberty Utilities Electricity Delivery Service Tariff – NHPUC No. 20:

https://www.puc.nh.gov/Regulatory/Docketbk/2018/18-183/INITIAL%20FILING%20-%20PETITION/18-183_2018-12-10_GSEC_TARIFF.PDF

New Hampshire Electric Co-op Net Metering Requirements:

<https://www.nhec.com/wp-content/uploads/2017/02/2017-Interconnection-Application-Package.pdf>

Public Service Company of New Hampshire Interconnection Standards for Inverters Sized Up to 100 KVA, August 2009:

https://www.eversource.com/content/docs/default-source/builders-contractors/eversource's-interconnection-standards-for-inverters.pdf?sfvrsn=2dd9cf62_0

Unitil Energy Systems, Inc. Interconnection Standards for Inverters Sized up to 100 kVA:

https://unitil.com/sites/default/files/pdfs/UES%20100%20KVA%20Interconnect%20Standard%202009_08_21_1.pdf

Rhode Island –

State of Rhode Island Public Utilities Commission and Division of Public Utilities and Carriers

Block Island Power Company Net Metering Application:

<https://blockislandpowercompany.com/net-metering-application-2/>

The Narragansett Electric Company Standards for Connecting Distributed Generation, Effective September 6, 2018:

https://www9.nationalgridus.com/non_html/RI_DG_Interconnection_Tariff.pdf

Pascoag Utility District – Electric Net Metering Policy, Requested Effective Date: June 1, 2010:

<https://www.pud-ri.org/wp-content9999/uploads/2015/07/Net-Metering-Policy.pdf>

Vermont –

Vermont Public Utility Commission

The Vermont Public Utility Commission issued an interconnection rule in 2006 that was largely modeled on the FERC Small Generator Interconnection Procedures at that time. The rule has not been updated since 2006.

Links to the current rule as well as an application form and application instructions:

PUC Rule 5.500 – Interconnection Rule

https://puc.vermont.gov/sites/psbnew/files/doc_library/5500-electric-generation-interconnection-procedures_0.pdf

PUC Rule 5.500 – Application Form

https://puc.vermont.gov/sites/psbnew/files/doc_library/5500-revised-application_0.pdf

PUC Rule 5.500 – Application Instructions

https://puc.vermont.gov/sites/psbnew/files/doc_library/5500-revised-application-instructions_0.pdf

In addition, the Department petitioned the PUC to initiate a rulemaking to make adjustments to the interconnection rule in 2016. As of the date of this DER Guidance document there were some filings and a workshop, but the process recently ended without resolution. The PUC has indicated that they are likely to take up the process again in the near future however has not provided NPCC with a date. Information regarding this process can be found here: <https://puc.vermont.gov/about-us/statutes-and-rules/proposed-changes-rule-5500>

Province of Quebec (some references are only available in French)

Section 112 of the [Act respecting the Régie de l'énergie](#) (chapter R-6.01) (the Act) reads as follows:

112. THE GOVERNMENT MAY MAKE REGULATIONS DETERMINING

[...]

(2.1) *for a particular source of electric power supply, the corresponding energy block and maximum price established for the purpose of fixing the cost of electric power referred to in section 52.2 or for the purposes of the supply plan provided for in section 72, or for the purposes of a tender solicitation by the electric power distributor under section 74.1;*

(2.2) *the timeframe applicable to a public tender solicitation by the electric power distributor under section 74.1;*

(2.3) *the maximum production capacity referred to in section 74.3, which may vary with the source of renewable energy or the class of customers or producers specified;*

[...]

In cases where energy needs are to be supplied out of an energy block, a regulation may provide that only certain classes of suppliers may be invited to tender by the electric power distributor and that the quantity of electric power required under each supply contract may be limited.

Consequently, the Government has taken the following regulations, regarding Distributed Energy Resources (or DER), between 2003 and 2013:

- [CONCERNANT le Règlement sur l'énergie produite par cogénération](#) (Décret 1319-2003, 10 décembre 2003);
- [CONCERNANT le Règlement sur l'énergie éolienne et sur l'énergie produite avec de la biomasse](#) (Décret 352-2003, 5 mars 2003);
- [CONCERNANT le Règlement modifiant le Règlement sur l'énergie produite par cogénération](#) (Décret 298-2004, 29 mars 2004);
- [CONCERNANT le Règlement sur le second bloc d'énergie éolienne](#) (Décret 926-2005, 12 octobre 2005);
- [CONCERNANT le Règlement sur l'énergie produite par cogénération à la biomasse](#) (Décret 916-2008, 24 septembre 2008);
- [CONCERNANT le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets autochtones](#) (Décret 1043-2008, 29 octobre 2009);
- [CONCERNANT le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 1045-2008, 29 octobre 2008);
- [CONCERNANT le Règlement modifiant le Règlement sur l'énergie produite par cogénération à la biomasse](#) (Décret 9-2009, 7 janvier 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 179-2009, 4 mars 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets autochtones](#) (Décret 180-2009, 4 mars 2009);
- [CONCERNANT le Règlement sur la capacité maximale de production visée dans un programme d'achat d'électricité pour des petites centrales hydroélectriques](#) (Décret 336-2009, 25 mars 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets autochtones](#) (Décret 520-2009, 29 avril 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 521-2009, 29 avril 2009);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 468-2010, 2 juin 2010);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets autochtones](#) (Décret 469-2010, 2 juin 2010);
- [CONCERNANT le Règlement sur la capacité maximale de production visée dans un programme d'achat d'électricité produite par cogénération à base de biomasse forestière résiduelle](#) (Décret 1085-2011, 26 octobre 2011);
- [CONCERNANT le Règlement sur un bloc de 450 mégawatts d'énergie éolienne](#) (Décret 1149-2013, 6 novembre 2013).

The following regulations, or modified regulations (marked in yellow highlight in the section above) have led to four tender solicitations, targeting precise quantities, or energy blocks, of wind Energy:

- [CONCERNANT le Règlement sur l'énergie éolienne et sur l'énergie produite avec de la biomasse](#) (Décret 352-2003, 5 mars 2003);

- [CONCERNANT le Règlement sur le second bloc d'énergie éolienne](#) (Décret 926-2005, 12 octobre 2005);
- [CONCERNANT le Règlement modifiant le Règlement sur un bloc de 250 MW d'énergie éolienne issu de projets communautaires](#) (Décret 468-2010, 2 juin 2010);
- [CONCERNANT le Règlement sur un bloc de 450 mégawatts d'énergie éolienne](#) (Décret 1149-2013, 6 novembre 2013).

The Régie considers the results of these tenders when examining Hydro-Québec's supply plan, as per section 72 of the Act:

72. *With the exception of private electric power systems, a holder of exclusive electric power or natural gas distribution rights shall prepare and submit to the Régie for approval, according to the form, tenor and intervals fixed by regulation of the Régie, a supply plan describing the characteristics of the contracts the holder intends to enter into in order to meet the needs of Québec markets following the implementation of the energy efficiency measures. The supply plan shall be prepared having regard to*

- (1) the risks inherent in the sources of supply chosen by the holder;*
- (2) as concerns any particular source of electric power, the energy block established by regulation of the Government under subparagraph 2.1 of the first paragraph of section 112; and*

[...]

When examining a supply plan for approval, the Régie shall consider such economic, social and environmental concerns as have been identified by order by the Government.

Sections 74.1 and 74.2 of the Act provide that the Régie oversees the process of such tender solicitations:

74.1. *To ensure that suppliers responding to a tender solicitation are treated with fairness and impartiality, the electric power distributor shall establish and submit for approval to the Régie, which shall make its decision within 90 days, a tender solicitation and contract awarding procedure and a tender solicitation code of ethics applicable to the electric power supply contracts required to meet the needs of Québec markets in excess of the heritage pool, or the needs to be supplied out of an energy block determined by regulation of the Government under subparagraph 2.1 of the first paragraph of section 112.*

The tender solicitation and contract awarding procedure shall, in particular,

- (1) allow all interested suppliers to tender by requiring the tender solicitation to be issued in due time;*
- (2) grant equal treatment to all sources of supply and energy efficiency projects unless the tender specifications provide that all or part of the needs met by a particular source of supply must be supplied out of an energy block determined by regulation of the Government;*
- (3) favour the awarding of supply contracts based on the lowest tendered price for the required quantity of electric power and in keeping with the required conditions, taking into account the applicable transmission cost and, where the tender specifications provide that all or part of the needs met by a particular source of supply must be supplied out of an energy block, taking into account the maximum price established by regulation of the Government; and*
- (4) provide that, following a tender solicitation, contracts may be awarded to two or more suppliers, in which case a supplier offering the required quantity of electric power may be invited to reduce the quantity offered without modifying the tendered unit price.*

An energy efficiency project to which a tender solicitation applies under subparagraph 2 of the second paragraph must meet the stability, sustainability and reliability requirements that apply to conventional sources of supply.

The Régie may dispense the electric power distributor from soliciting tenders for short-term contracts or where urgent needs must be met.

For the purposes of this section, the promoter of an energy efficiency project is deemed to be an electric power supplier.

74.2. *The Régie shall monitor the implementation of the tender solicitation and contract awarding procedure and code of ethics provided for in section 74.1 and ascertain whether they are complied with. To that end, the Régie may require any document or information it considers useful. The Régie shall report its findings to the electric power distributor and to the supplier chosen.*

The electric power distributor may not enter into an electric power supply contract unless it has obtained the approval of the Régie, under the conditions and in the cases determined by regulation by the Régie.

The Régie's Website lists every docket related to this jurisdiction over Québec's electricity distributor (in French only): [Approval of supply contracts](#).

The Régie also considers DER when adopting specific reliability standards. Sections 85.2 and 85.7 of the Act read as follows:

85.2. *The Régie shall ensure that electric power transmission in Québec is carried out according to the reliability standards it adopts.*

85.7. *The Régie may request the reliability coordinator to modify a standard filed or submit a new one, on the conditions it sets. It shall adopt reliability standards and set the date of their coming into force.*

The reliability standards may

- (1) subject to section 85.10, provide for a schedule of sanctions, including financial penalties, that apply if standards are not complied with; and*
- (2) refer to reliability standards set by a standardization agency that has entered into an agreement.*

Docket [R-4070-2018](#) (in French only) relates to a request by the reliability coordinator (HQCME) and is still under examination by the Régie. It aims the adoption of reliability standards associated with Special Protection System (Remedial Action Scheme) and Dispersed Power Producing Resources.

The following sections of Québec' electricity distributor and transmitter's web site might be useful, since they list the applicable technical codes, standards and requirements:

- http://www.hydroquebec.com/transenergie/fr/commerce/raccordement_distribution.html ;
- http://www.hydroquebec.com/transenergie/fr/commerce/raccordement_transport.html

Province of Ontario

The current connection requirements for all resources can be found in Chapter 4 appendices 4.2 and 4.3 of the Market Rules. <http://www.ieso.ca/-/media/Files/IESO/Document-Library/Market-Rules-and-Manuals-Library/market-rules/mr-chapter4appx.pdf?la=en>

The Independent Electric System Operator (IESO) is in the process of making updates to these requirements to be more specific about the requirements that apply to all DERs (not just storage). <http://www.ieso.ca/Sector-Participants/Engagement-Initiatives/Engagements/Updates-to-Performance-Requirements-Market-Rule-Appendices-4-2-and-4-3>

The IESO is working on several white papers. The one that was posted in 2019 called "**Exploring Expanded DER Participation in the IESO-Administered Markets**" sets out the participation models that exist for DER in wholesale markets in general and in the IESO-Administered Markets (IAM) today and

also identify the range of options that exist for expanded participation in the future. In addition, this paper provides a working definition of DER, sets out principles for integrating them into wholesale markets, offers an initial review of participation models in other jurisdictions, and identifies key barriers that may limit DER participation in the IAMs.

<http://www.ieso.ca/-/media/Files/IESO/Document-Library/White-papers/White-paper-series-Conceptual-Models-for-DER-Participation.pdf?la=en>

The Ontario Energy Board is also engaging in several stakeholder activities in this area. Below are the links to those activities. The Ontario Energy Board has combined the first two initiatives into one engagement.

1. **Responding to Distributed Energy Resources (DER)*** - The purpose of this initiative is to develop a more comprehensive regulatory framework that facilitates investment and operation of DER based-on value to consumers and supports effective DER integration so the benefits of sector evolution can be realized.

<https://www.oeb.ca/industry/policy-initiatives-and-consultations/responding-distributed-energy-resources-ders>

2. **Utility Remuneration*** - The purpose of this initiative is to identify how to remunerate utilities in ways that make them indifferent to traditional or innovative solutions, better supports their pursuit of least cost solutions, strengthens their focus on long-term value and requires them to reflect the impact of sector evolution in their system planning and operations.

<https://www.oeb.ca/industry/policy-initiatives-and-consultations/utility-remuneration>

3. **DER Connections Review** – The purpose of this initiative to review its requirements regarding the connection of distributed energy resources (DER) by licensed electricity distributors. The purpose of this initiative is to identify any barriers to the connection of DER, and where appropriate to standardize and improve the connection process. The review will be focused on connection of electricity generation and storage facilities connected to the distribution system, either in front or behind the distributor's meter.

<https://www.oeb.ca/industry/policy-initiatives-and-consultations/distributed-energy-resources-der-connections-review>

The contact for this information would be Customer Relations (customer.relations@ieso.ca)

Province of New Brunswick

Within the province, DER is referred to as “Embedded Generation” or “Distributed Generation.” Regulation from the New Brunswick Energy and Utility Board may be found here:

<http://laws.gnb.ca/en/ShowPdf/cs/2013-c.7.pdf>

Énergie NB Power’s embedded generation may be found here:

<https://www.nbpower.com/en/products-services/embedded-generation/>

Appendix F, ISO New England

ISO-NE specific Inverter requirements are as follows in the below table and the link

[Inverter Source Requirement Document of ISO New England](#)

The following additional performance requirements are applied in one NPCC Area and are provided as an example:

- In the Permissive Operation region above 0.5 p.u., inverters shall ride-through in Mandatory Operation mode, and
- In the Permissive Operation region below 0.5 p.u., inverters shall ride-through in Momentary Cessation mode.

Table I: Inverters' Voltage Trip Settings

Shall Trip – IEEE Std 1547-2018 (2 nd ed.) Category II					
Shall Trip Function	Required Settings		Comparison to IEEE Std 1547-2018 (2 nd ed.) default settings and ranges of allowable settings for Category II		
	Voltage (p.u. of nominal voltage)	Clearing Time(s)	Voltage	Clearing Time(s)	Within ranges of allowable settings?
OV2	1.20	0.16	Identical	Identical	Yes
OV1	1.10	2.0	Identical	Identical	Yes
UV1	0.88	2.0	Higher (default is 0.70 p.u.)	Much shorter (default is 10 s)	Yes
UV2	0.50	1.1	Slightly higher (default is 0.45 p.u.)	Much longer (default is 0.16 s)	Yes

Table II: Inverters' Frequency Trip Settings

Shall Trip Function	Required Settings		Comparison to IEEE Std 1547-2018 (2 nd ed.) default settings and ranges of allowable settings for Category I, Category II, and Category III		
	Frequency (Hz)	Clearing Time(s)	Frequency	Clearing Time(s)	Within ranges of allowable settings?
OF2	62.0	0.16	Identical	Identical	Yes
OF1	61.2	300.0	Identical	Identical	Yes
UF1	58.5	300.0	Identical	Identical	Yes
UF2	56.5	0.16	Identical	Identical	Yes

Table III: Inverters' Voltage Ride-through Capability and Operational Requirements

Voltage Range (p.u.)	Operating Mode/ Response	Minimum Ride-through Time(s) (design criteria)	Maximum Response Time(s) (design criteria)	Comparison to IEEE Std 1547-2018 (2 nd ed.) for Category II
$V > 1.20$	Cease to Energize	N/A	0.16	Identical
$1.175 < V \leq 1.20$	Permissive Operation	0.2	N/A	Identical
$1.15 < V \leq 1.175$	Permissive Operation	0.5	N/A	Identical
$1.10 < V \leq 1.15$	Permissive Operation	1	N/A	Identical

$0.88 \leq V \leq 1.10$	Continuous Operation	infinite	N/A	Identical
$0.65 \leq V < 0.88$	Mandatory Operation	Linear slope of 8.7 s/1 p.u. voltage starting at 3 s @ 0.65 p.u.: $T = 3 \text{ s} + \frac{8.7 \text{ s}}{V - 0.65 \text{ p.u.}}$ VRT 1 p. u.	N/A	Identical
$0.45 \leq V < 0.65$	Permissive Operation ^{a,b}	0.32	N/A	See footnotes a & b
$0.30 \leq V < 0.45$	Permissive Operation ^b	0.16	N/A	See footnote b
$V < 0.30$	Cease to Energize	N/A	0.16	Identical

The following additional operational requirements can be used. Provided as an example:

- In the Permissive Operation region above 0.5 p.u., inverters shall ride-through in Mandatory Operation mode, and
- In the Permissive Operation region below 0.5 p.u., inverters shall ride-through in Momentary Cessation mode with a maximum response time of 0.083 seconds.

Table IV: Inverters' Frequency Ride-through Capability

Frequency Range (Hz)	Operating Mode	Minimum Time(s) (design criteria)	Comparison to IEEE Std 1547-2018 (2 nd ed.) for Category II
$f > 62.0$	No ride-through requirements apply to this range		Identical
$61.2 < f \leq 61.8$	Mandatory Operation	299	Identical
$58.8 \leq f \leq 61.2$	Continuous Operation	Infinite	Identical
$57.0 \leq f < 58.8$	Mandatory Operation	299	Identical
$f < 57.0$	No ride-through requirements apply to this range		Identical

Table V: Grid Support Utility Interactive Inverter Functions Status

Function	Default Activation State
SPF, Specified Power Factor	OFF ²
Q(V), Volt-Var Function with Watt or Var Priority	OFF Default value: 2% of maximum current output per second
SS, Soft-Start Ramp Rate	ON
FW, Freq-Watt Function OFF	OFF

Appendix G, State Renewable and Green Energy Targets

New York State

70% renewable energy by 2030
85% reduction of Greenhouse Gas emissions by 2050
6,000 MW of distributed solar by 2025
3,000 MW of energy storage by 2025
Carbon free electricity system by 2040

Connecticut

Carbon free electricity system by 2040
Renewable Portfolio Standard - <https://portal.ct.gov/PURA/RPS/Renewable-Portfolio-Standards-Overview>

Vermont

90% of Vermont's overall energy needs from renewable sources by 2050
Reduce Vermont's greenhouse gas (GHG) emissions by 50% from the 1990 baseline level by 2028, and by 75% from the 1990 level by 2050

New Hampshire

20% to 25% reduction in Greenhouse Gas emissions by 2032
25.2% renewable energy by 2025

Rhode Island

100% renewable energy by 2030
1,000 MW of new clean energy installed in 2020

Maine

80% renewable energy by 2030

Appendix H, Autonomous Energy Grids

The National Renewable Energy Laboratory (NREL) and its partners are conducting research and development of advanced techniques that would enable the optimization and control of hundreds of millions of deployed distributed energy resources (DER). The concept known as “Autonomous Energy Grids (AEGs)” are multi-layer, or hierarchical, cellular-structured power grid and control systems that enable resilient, reliability, and economic optimization²⁸. Supported by a scalable, reconfigurable, and self-organizing information and control infrastructure, AEGs are extremely secure and resilient, and can operate in real time to ensure economic and reliable performance while systematically integrating energy in all forms. AEGs rely on cellular building blocks that can self-optimize when isolated from a larger grid and participate in optimal operation when interconnected to a larger grid. The figure H-1 shows how a scalable approach to control can be built from the lowest level of individual controllable technologies (renewable energy, conventional generation, electric vehicles, storage, and loads) and used to control hundreds of millions of devices through the use of hierarchical cells. To make this idea a reality, there are control algorithms for AEGs that will need to be developed and implemented with the following characteristics:

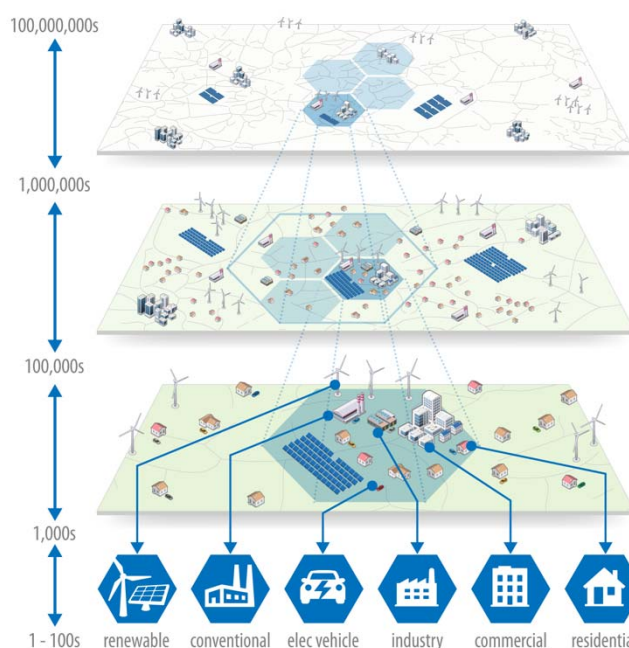


Figure H-1: Autonomous Energy Grids form a distributed hierarchical control system that integrated individual technologies in a cellular structure to the bulk power system.

- **Operate in Real Time** – Control algorithms must operate fast enough to ensure real-time operations in power grids that balance load and generation every second.
- **Handle Asynchronous Data and Control Actions** – Data needs to be used from a variety of asynchronous measurements and sources; whereas distributed decision-making leads to asynchronous control actions.
- **Robustness** – This covers both reliability and resilience, where reliability is fault tolerance and resilience are the ability to come back from a failed state. These control systems must also be

²⁸ “Autonomous Energy Grids”, B. Kroposki, E. Dall’Anese, A. Bernstein, Y. Zhang, B. Hodge, Proceedings of the 51st Hawaii International Conference on System Sciences, January 2018, <https://scholarspace.manoa.hawaii.edu/bitstream/10125/50229/1/paper0342.pdf>

robust to communications failures, prolonged communications outages, and large-scale disturbances.

- **Scalable**— Control algorithms must operate in a scalable fashion to ensure control of hundreds of millions of devices.

NREL has evaluated the AEG algorithms on both large-scale laboratory testing and small-scale real-world demonstrations. NREL evaluated the algorithms as part of the DOE ARPA-E NODES program that demonstrated the first implementation of the algorithms in hardware and successfully demonstrate real-time optimization of a single AEG cell with more than 100 controllable devices at NREL's Energy Systems Integration Facility²⁹. The experiment includes simulation of a real distribution feeder from California with 366 single-phase connection points, more than 100 controllable assets at power (inverters, electric vehicles, and batteries), and hundreds of simulated devices. The distributed algorithms were implemented in cost-effective microcontrollers that self-optimize and communicate to the central coordinator to attain system-wide goals (voltage regulation, frequency response).

NREL has also moved out of the lab to demonstrate the deployment of AEGs in the real world. The team has been working with Holy Cross Energy (HCE), a utility cooperative near Aspen, Colorado, to deploy the AEG technology in a group of smart homes in Basalt, CO³⁰. The smart homes in Basalt Vista are a pilot for an altogether new approach to the grid. These homes optimize energy for residents and their neighbors, but the principles behind Basalt Vista go much further. Within homes, each new connected device or energy resource like a residential battery, water heater, or solar photovoltaic (PV) system, can be controlled for unprecedented energy efficiency. And at a larger scale, entire communities could rapidly share power, creating reliable energy for everyone.

²⁹ <https://www.nrel.gov/news/features/2019/from-the-bottom-up-designing-a-decentralized-power-system.html>

³⁰ <https://www.nrel.gov/news/features/2019/small-colorado-utility-sets-national-renewable-electricity-example-using-nrel-algorithms.html>



Recent FERC Activities

Kal Ayoub

Deputy Director, Division of Cyber Security, Office of Electric Reliability

Federal Energy Regulatory Commission

May 12, 2021

The views expressed in this presentation are my own and do not represent those of the Commission or any individual Commissioner

Technical Conferences and Workshop

Office of Public Participation Workshop and Listening Sessions

Docket No. AD21-9-000.

- In 12/2020, Congress directed the Commission to provide a report, by 6/25/2021, detailing its progress towards establishing the OPP. Section 319 of the Federal Power Act directs the Commission to establish the OPP to “coordinate assistance to the public with respect to authorities exercised by the Commission,” including assistance to those seeking to intervene in Commission proceedings. (16 U.S.C. § 825q–1).
- Purpose of the workshop and listening sessions was to solicit public input on how the Commission should establish and operate the Office of Public Participation (OPP) pursuant to section 319 of the Federal Power Act (FPA) (16 U.S.C. § 825q–1). The Commission is evaluating input from stakeholders.
- A report is due to Congress on 6/25/2021.

Electrification and the Grid of the Future

Docket No. AD21-12-000. Held 4/29/2021.

- Purpose of the conference is to initiate a dialog between Commissioners and stakeholders on how to prepare for an increasingly electrified future and discuss the shift from non-electric to electric sources of energy at the point of final consumption (e.g., to fuel vehicles, heat and cool homes and businesses, and provide process heat at industrial facilities).

Technical Conferences

Climate Change, Extreme Weather, and Electric System Reliability

Docket No. AD21-13-000. To be held on 6/1-2/2021 from 1pm - 5pm.

- Purpose of the conference is to discuss issues surrounding the threat to electric system reliability posed by climate change and extreme weather events, which are increasing in frequency, intensity, geographic expanse, and duration. As a result, the number and severity of weather-induced events in the electric power industry may also increase. It will also examine how grid operators prepare for and respond to extreme weather events, including, but not limited to droughts, extreme cold, wildfires, hurricanes, and prolonged heat waves.
- Comments in response to staff questions on threats to the electric system related to climate change and extreme weather events were due on 4/15/2021.

Western Resource Adequacy Conference

Docket No. AD21-14-000. To be held on 6/23-24/2021.

- Purpose of the conference is to discuss resource adequacy developments in the Western Interconnection from varied regional perspectives to discuss challenges, trends, and possible ways to continue to ensure resource adequacy in the Western Interconnection.

Reliability Technical Conference

Docket No. AD21-11-000. To be held on 9/30/2021.

- Purpose of the conference is to discuss policy issues related to the reliability of the Bulk-Power System. Supplemental notice on agenda to be issued in the future.

Joint Inquiry into 2021 Cold Weather Grid Operations

- On 2/16/2021, FERC and NERC announced a joint inquiry into the operations of the Bulk-Power System during the extreme winter weather conditions experienced by the Midwest and Southern Central states. The severe cold weather contributed to power outages affecting millions of electricity customers throughout the region.
- Chairman Glick stated that FERC will be "examining the root causes of . . . reliability events" that have occurred throughout the country, in particular in the regions served by ERCOT, SPP, and MISO.
- FERC and NERC will work with other federal agencies, states, regional entities and utilities to identify problems with the performance of the Bulk-Power System and, where appropriate, make recommendations for addressing those issues.
- Preliminary Findings and Recommendations:
Targeted: Late Summer 2021
- Final Report:
Targeted: Late Fall 2021

Recent Reliability Orders

Letter Order Approving Reliability Standards addressing supply chain risk management in Docket No. RD21-2-000.

- On 3/18/2021, the Commission approved several Reliability Standards revisions which expanded applicability to Electronic Access Control Monitoring System (EACMS) and Physical Access Control Systems (PACS) associated with high and medium impact BES Cyber Systems.
 - CIP-013-2 (Cyber Security – Supply Chain Risk Management)
 - CIP-005-7 (Cyber Security – Electronic Security Perimeter(s)), and
 - CIP-010-4 (Cyber Security – Configuration Change Management and Vulnerability Assessments).

Recent Reliability Orders

Delegated Letter approving Reliability Standard FAC-008-5 (Facilities Ratings), Docket No. RD21-4-000

- On 4/7/2021, the Commission approved the retirement of Requirement R7 from the current-version of the Reliability Standard.

Order Approving Reliability Standard BAL-002-WECC-3 (Contingency Reserve), Docket No. RM19-20-000

- On 4/15/2021, the Commission approved regional Reliability Standard BAL-002-WECC-3 (Contingency Reserve), which eliminates Requirement R2 from the prior version.
- Commission also directed NERC and WECC to submit an informational filing.

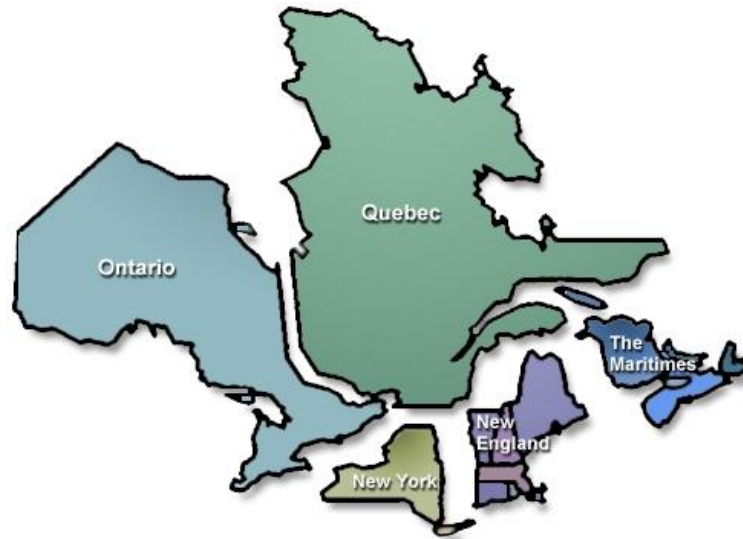
Get Vaccinated and Stay Safe!

- Thank you!
- Questions?



NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

NPCC Whitepaper on De-Carbonization Impacts, Identification and Prioritization of NPCC Reliability Directory Reviews due to Distributed Energy Resources (DER) and Variable Energy Resources (VER)



NPCC's Regional Standards Committee (RSC) and Reliability Coordinating Committee (RCC)
Endorsed XX/XX/2021

Note: Content of this document may not reflect the most current information. Periodic reviews for potential revisions of the document may be done at the request of the NPCC Board of Directors. Please send corrections or revision requests to [npccstandard@npcc.org](mailto:npscstandard@npcc.org).

Contributors:

Guy V. Zito	RSC Chair, NPCC Staff
Gerard Dunbar	NPCC Staff
Ruida Shu	NPCC Staff
Michael Jones	RCC and RSC Co-Vice Chair, National Grid
Herb Schrayshuen	Power Advisors, LLC
NPCC Task Forces	N/A

NPCC also thanks the Regional Standards Committee (RSC) and the State and Provincial regulatory authorities who provided guidance and information during the development of this whitepaper.

Revision History

Version	Date	Action	Change Tracking (New, Errata or Revisions)
1	XX/XX/21	Effective Date	New

Contents

Objective	5
NPCC Reliability Directories	6
Directory # 1 - Design and Operation of the Bulk Power System.....	7
Directory # 2 - Emergency Operations	8
Directory # 4 - System Protection Criteria	9
Directory # 5 - Reserve.....	10
Directory # 6 - Reserve Sharing Groups	11
Directory # 7 - Remedial Action Schemes	11
Directory # 8 - System Restoration.....	12
Directory # 11 - Disturbance Monitoring Equipment Criteria	12
Directory # 12 - Automatic UFLS Program Requirements.....	12
Directory Prioritization Recommendation	13
Appendix A- Future Directory Review Considerations	14
Appendix B- Decarbonization Goals within NPCC.....	15

Executive Summary

The development of this document was initiated by the NPCC Board of Directors to provide support, guidance, and information for use by NPCC Members and stakeholders. This whitepaper identifies recommended considerations and prioritization to manage the revision of NPCC Criteria located within each of the NPCC Reliability Directories¹. These revisions may be necessary because of increasing amounts of decarbonized Distributed Energy Resources (“DER”), and Variable Energy Resources (“VER”) being deployed or planned to be deployed due to de-carbonization goals within the NPCC Region.

Currently, within the NPCC region there are numerous state and provincial regulatory targets to achieve decarbonization goals. (See Appendix B). Additionally, several national laboratories and research organizations including EPRI, NYSERDA, and the National Renewable Energy Laboratory are actively considering issues surrounding decarbonization.

As DER and VER continue to replace traditional industry generation resources the resource fuel mix and operational characteristics of the system will fundamentally change and necessitate changes to how the system is planned and operated.

Simulating the usual cases and contingencies in transmission planning and operations will no longer be adequate to capture the impact created by DER and these functions (planning and operations) will need to reinvent themselves to address new issues such as ramping and inertia. Other concerns such as data collection by Distribution Providers, transmission protection philosophy and study tools employed for analysis will also need to be addressed.

Additionally, the North American Electric Reliability Corporation (NERC) Reliability Standards are not applicable to equipment on the distribution systems unless such equipment has a direct impact on the “reliable operation”² of the BPS, such as Automatic Underfrequency Load Shedding (UFLS). However, as penetration of DER and VER increases, planning and operating assessments used to assure the reliable operation of the BPS will need to accurately represent how DER and VER, interact with the BPS and NPCC’s Criteria contained the NPCC Reliability Directories may need to be revised or augmented.

NPCC recognizes that continent-wide efforts in North America are underway at the NERC level to define DER and VER and to address some aspects related to planning and modeling. The NERC LTRA (Long Term Reliability Assessment) which is developed annually by NERC, recognizes the unprecedented transformational changes underway in the electricity sector and provides a summary of current efforts underway to address these emerging risks. There are specific reliability activities related to DER being conducted by the NERC System Planning Impacts from Distributed Energy Resources Working Group (“SPIDERWG”), and Inverter-Based Resource and Performance Working Group (“IRPWG”).

NPCC Staff and its members have been actively participating in these continent-wide efforts and are contributing to the work underway to address outstanding issues within the scope of those groups. With the understanding of current ongoing efforts, NPCC can fill an important role by identifying additional areas where the Region may provide information and services and revise the existing NPCC

¹ NPCC Directories contain requirements which are expected to be met by NPCC Full Members as is applicable to their functions in maintaining the reliability of the NPCC Bulk Power System.

² “reliable operation” is defined in 16 U.S. Code § 824o and means “operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.”

Criteria to promote the reliable deployment of DER and VER. Such opportunities exist in the areas of data acquisition, modeling, testing and verification, observability, protection systems and other operational characteristics of DER and VER.

Although the purpose of this NPCC whitepaper is not to create new Criteria or Standards, it is recognized that the review of the Directories may result in a need to add Criteria such as for energy sufficiency. The intent of this document is to utilize and analyze information to make recommendations on prioritizing reviews of NPCC criteria for potential DER impact. Concurrent with NPCC's revisions of the Reliability Directories, NERC's SPIDERWG and other groups are developing guidance documents and NPCC will continue to consider NERC guidance documents during the Directory review process to achieve continued alignment and avoid duplication.

This whitepaper contains a prioritization of Directory reviews and categorizes them (low medium or high) using the input on the potential impact of the DER and VER, provided by NPCC's Members, NERC, the industry, and Staff observations during the NPCC DER VER Forums. Accordingly, there are two NPCC Regional Reliability Directories that this whitepaper recommends as 'high priority' or 'high to moderate ' priority for review: Directory # 1 *"Design and Operation of the Bulk Power System"* and Directory # 4 *"Bulk Power System Protection Criteria"*. Directory # 1 has entered into the revision process and the project Scope document contains review of DER and VER potential impacts on NPCC Criteria.

Objective

The objective of this effort is to conduct a review of NPCC's Criteria in the Directories for potential impacts of DER and VER deployment and not to conduct an exhaustive review of each Directory. DER and VER deployment and technologies continue to be developed and implemented and this whitepaper is meant only as guidance based on what NPCC and its members anticipate at the time of its writing.

Unlike large transmission-connected generation facilities, DER facilities often do not provide essential grid reliability services (although some are technically capable of doing so). Some DER, classified as VER, are also inherently intermittent in nature and the introduction of these intermittent resources has resulted in increasing amounts of energy storage. Although, pumped storage technology has been available to power systems for many decades, there are challenges to the development of new pumped storage facilities and new battery-based storage technology is under active development and significant deployment. The framework for operating storage is currently undergoing significant debate and discussion. Modes of operation from peak shaving, essential reliability ancillary services, and time-of-day energy arbitrage are also under development. Any NPCC Directory changes which can be made to accommodate the evolution of storage technology or remove any perceived impediments to deployment of battery energy storage systems should be considered during Directory reviews.

For the purpose of this NPCC guidance whitepaper, DER refers to:

Any non-BPS or non -BES connected real or reactive power resources (generating units, multiple generating units at a single location, distributed generation installations, battery storage systems, etc.) located within the boundary of any distribution utility's service territory, regardless

of capacity,,. Some DER technologies are more intermittent in their production characteristics than resources that operate based on a controllable fuel input.

For the purpose of this NPCC guidance whitepaper, VER refers to:

An energy resource that: has primary energy source variability that is beyond the full control of the facility owner or operator.

In this whitepaper, NPCC will also leverage work in progress by the SPIDERWG. NPCC Staff has been participating in a sub-group of the SPIDERWG to analyze all NERC Reliability Standards, including the Operation and Planning Standards, for potential DER Impact. However, as part of the SPIDERWG analysis, Cyber Security Standards were not evaluated. The relationship of each NPCC Directory to specific recommendations provided for the associated NERC Standards was considered in the recommendations along with additional issues that may impact the NPCC Region. Also considered was the recent FERC order (Order 2222) on allowing individual DER aggregations as low as 100 kW to participate in wholesale markets in the US. Although such aggregation improves visibility and control, the effect of aggregation can have a significant effect on the power system and if not properly understood can impact the reliable operation of the BPS, as seen in California, where resource planning targets have not kept pace with the evolving power mix, and demand during peak hours outpaces the supply of solar-produced power. NPCC is now beginning to observe aggregations of DER entering into the capacity wholesale markets and has considered those potential impacts in this summary. The suggested priorities in this whitepaper for the review of Directory criteria may need to be modified as emerging issues related to DER and VER deployment, interconnection, planning, and operations are identified, and their technology continues to improve.

Upon determination of the potential impact of DER and VER, with the considerations given to past work done, NPCC is providing a recommendation on prioritizing the review of each Directory. Each Directory is reviewed for revision on a three-year cycle. However, there may be a need to reprioritize the review and potential revision of a Directory based on need. For the purposes of this analysis, it is recommended that consideration be given to immediately begin a review on Directory #1 *Design and Operation of the Bulk Power System* (currently initiated with Scope developed). Additionally, a focused review of Directory # 4 *System Protection Criteria* to consider emerging protection issues is also recommended. These two Directories will have the most immediate impact because of DER and VER in the NPCC Region.

NPCC Reliability Directories

The requirements of an NPCC Directory apply only to those facilities defined as NPCC bulk power system elements as identified through the performance-based methodology of NPCC Document A-10 *Classification of Bulk Power System Elements* the current list of which is maintained by the NPCC Task Force on System Studies and approved by the NPCC Reliability Coordinating Committee.

The potential reliability impact of increased penetration of Distributed Energy Resources, and Variable Energy Resources (VER) provide a unique opportunity for NPCC Members to utilize the NPCC Task Forces

and Working Groups to identify opportunities to enhance the criteria and address emerging risks which may be outside the jurisdiction of FERC and the NERC Reliability Standards.

As the penetration of DER and VER increases, a recognition that facilities on the distribution system and not on the BPS are impacting the planning and operating assessments contained in the criteria will be critical.

Resource variability, limited large-scale on-demand response, decreased short-circuit strength, load offset, flow direction changes, frequency stability, and UFLS effectiveness present an opportunity to strategically enhance the NPCC criteria to address these DER related issues.

NPCC currently maintains nine Regional Reliability Directory documents, each containing NPCC's reliability Criteria. Directory # 12 is scheduled to be retired in 2021 due to the adoption of NPCC's Regional Standard on Automatic UFLS, PRC-006-NPCC-2, by all the applicable governmental authorities across the NPCC Region. Therefore Directory # 12 was not considered in this analysis.

Details of the review and findings of each Directory for potential DER and VER impact appear below:

Directory # 1 - Design and Operation of the Bulk Power System

Applicable NERC Standards-

- EOP-011- Emergency Operations
- FAC-011- System Operating Limits Methodology for the Operating Horizon
- IRO-002- Reliability Coordination Monitoring and Analysis
- IRO-014- Coordination Among Reliability Coordinators
- MOD-031- Demand and Energy Data
- MOD-032- Data for Power System Modelling and Analysis
- TOP-001- Transmission Operations
- TOP-002- Operations Planning
- TOP-003- Operational Reliability Data
- TPL-001- Transmission System Planning Performance Requirements
- VAR-001- Voltage and Reactive Control

Determination of Impact from DER and VER:

Responsible entities may need to consider DER data in their long-term operational planning considerations. As large amounts of DER and VER are integrated as part of the power system, certain additional conditions may need to be addressed in the planning and operational reviews specified in Directory#1. For example, the addition of large amounts of DER solar resources may lead to mid-day minimum load conditions, which can be significantly lower than previously observed nighttime minimum load conditions, and which can impact other modeling parameters such as the bus-by-bus load distribution .

Existing requirements are applicable to "Small non-dispatchable DERs" connected to the bulk electric system; however, these requirements may be insufficient in the future for planning and operation with large amounts of DER. Likewise, although some voltage and frequency withstand/ride-through

capabilities specified in IEEE Std 1547-2018 currently apply, they may not be sufficiently specific, and the criteria could address such a gap.

There may also be a need for additional focus on how well Remedial Action Schemes (RAS) are coordinated with DER, particularly as more DER is deployed on the system. The SPIDERWG has issued guidelines to specify DER data requirements more granularly to capture the operational characteristics of DER and VER and require Distribution Providers to obtain and make available DER data, specifically, pertaining to aggregations, and reactive capabilities at a minimum. However, NPCC should review the Directories in the context of the absence of this requirement in NERC Standards and consider the difficulty for Planning Coordinators and Transmission Planners to obtain the necessary data from Distribution Providers.

Additionally, the loss of short circuit strength associated with the increased penetration of DER and VER along with the retirement of base generation and severe weather assumptions because of new technology (VER) could be considered in a review of Directory#1 .

Due to the uncertain nature of DER and VER, the methodologies used to determine operating limits may not be accurate. The uncertainty of DER has a larger impact with increasing penetration of DER. Therefore, a consideration for new or clarified Criteria and methodologies may be needed to account for this uncertainty. The increasing penetration of DERs will likely require additional focus from Reliability Coordinators to when determining operating limits. This may be done at the NERC level but NPCC should be cognizant of this potential effect on operations.

Finally, any review of Directory#1 to review the impact of DER and VER should consider both current and proposed methods of determining resource adequacy.

Directory # 2 - Emergency Operations

Applicable NERC Standards-

- BAL-002- Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event
- BAL-003- Frequency Response and Frequency Bias
- BAL-005- Automatic Generation Control
- EOP-011- Emergency Operations
- IRO-009- Reliability Coordinator Actions to Operate Within IROLs
- TOP-001- Transmission Operations
- TOP-002- Operations Planning

Determination of Impact from DER and VER:

It is important to understand that Balancing Authorities must understand all impacts, not just DER and VER, on balancing and regulating needs to meet the performance requirements of BAL-002 *“Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event.”* Year-over-year reviews of Balancing Authorities have shown consistent performance to the Standards and Criteria. DER and VER need to be considered in the emergency operating plans insofar as how these resources are used to avoid emergency conditions (DER shouldn't be curtailed during an energy emergency), and that under-frequency load shedding is not made ineffective by lack of DER visibility. As DER penetration continues to increase it may become necessary to have adaptive UFLS systems in place in the future. There is a benefit to consider providing the industry with guidance on considering DERs in UFLS studies and providing recommended practices for studies of gross load versus net load. Further consideration of how UFLS programs should be coordinated with DER's ride-through capability and there is also importance to modeling gross load and aggregate DER in under frequency load shedding (UFLS) simulations to ensure representation of the actual behavior of the BPS.

The increased amounts of DER and associated data will need to be considered in the Real-time analysis process. DER data will have no precedence over any other data gathered in the evaluation process conducted by the Reliability Coordinator. However, if the DER is identified as impactful to a system operating limit, the Reliability Coordinator should make every effort to coordinate with the appropriate distribution entities per the IEEE 1547 Standard (which may require the RC to change their methodology slightly to include the IEEE 1547 Standard language). Likewise, there may be an opportunity to achieve regional agreement within the criteria on protection issues to prevent issues such as observed in California. Transmission and Distribution entities must follow the Operating Instructions received from their Reliability Coordinator, regardless of whether DER or VER operation was a factor in the limit, unless the entity provides a reliability reason for non-compliance. Furthermore, existing Standard requirements already address the next day Real-time evaluation for the System Operating Limit (SOL) as well as the Interconnection Reliability Operating Limits (IROLs).

Directory # 4 - System Protection Criteria

Applicable NERC Standards-

- PRC-001- System Protection Coordination
- PRC-002- Disturbance Monitoring and Reporting Requirements
- PRC-004- Protection System Misoperation Identification and Correction
- PRC-005- Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance
- PRC-006- Automatic Underfrequency Load Shedding
- PRC-010- Undervoltage Load Shedding
- PRC-012- Remedial Action Schemes
- PRC-018- Disturbance Monitoring Equipment Installation and Data Reporting
- PRC-019- Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

- PRC-023- Transmission Relay Loadability
- PRC-024- Generator Frequency and Voltage Protective Relay Settings
- PRC-025- Generator Relay Loadability
- PRC-026- Relay Performance During Stable Power Swings
- PRC-027- Coordination of Protection Systems for Performance During Faults (Future enforcement)
- FAC-008- Facility Ratings

Determination of Impact from DER and VER:

Although the criteria in Directory#4 presently focuses more on protection system design and independence, rather than specific criteria for relay settings, DER and transmission connected VER issues will likely impact considerations surrounding relay protection settings in the future.

As DER continues to be deployed in the Region there are instances where distribution feeders are back-feeding into the Transmission System creating design issues for protective relays and other control devices which may be designed for directional flows.

Additionally, as more and more transmission level generators come offline, decreasing levels of fault current will need to be considered to ensure that relay protection can operate as designed.

Finally, the deployment of advanced Inverter functions and “grid forming” inverters may require a greater level of system protection coordination.

Directory # 5 - Reserve

Applicable NERC Standards

- BAL-002- Disturbance Control Standard: Contingency Reserve for Recovery from a Balancing Contingency Event
- BAL-005- Automatic Generation Control
- EOP-011- Emergency Operations

Determination of Impact from DER and VER:

The Criteria itself may not need revision for DERs and VERs, but a consistent and uniform approach regarding DERs (e.g., counting DERs either explicitly as resources or implicitly as load modifiers) may be needed. A review of the Criteria in the context of further deployment of these resources would be helpful, and any associated potential Glossary changes/additions may also be an effective way to implement consistent treatment from a Regional perspective. Reporting of net generation and net load will be affected by how DER is counted and the resultant apportionment of Interconnection Frequency Response Obligation (“IFRO”) to each BA. Consideration should be given to address counting and capacity of DERs consistently. NERC Reliability Subcommittee is currently reviewing this.

Directory # 6 - Reserve Sharing Groups

Applicable NERC Standards

- BAL-002- Disturbance Control Standard: Contingency Reserve for Recovery from a Balancing Contingency Event

Determination of Impact from DER and VER:

NPCC's Directory #6 includes specific requirements for types of spinning reserve. These reserves were specified to support the NPCC Region meeting the BAL-002 standard as it relates to returning Area Control Error to pre-contingency levels in specific recovery periods. As DER increases there will be less inertia on the system which may necessitate a review of the required spinning reserve assignments. Although, DER and VER may eventually play a role in system reserve, at this time an immediate review of this issue is not required.

Directory # 7 - Remedial Action Schemes

Applicable NERC Standards

- PRC-012 - Remedial Action Schemes
- PRC-017- Remedial Action Scheme Maintenance and Testing

Determination of Impact from DER and VER:

In general, this Directory specifies a process of implementation and periodic assessment of RAS. The process does not need to change with increasing levels of DERs or VER. The RAS may include tripping/shedding of a large amount of load, which is typically implemented with the tripping of feeder breakers in a distribution substation. If the presence of DERs is negligible, there may be little risk to BES reliability if DERs are also tripped with the load. However, in geographical areas with high penetration of DERs, loss of DERs due to automatic underfrequency load shedding or RAS activated load shedding may have an impact on grid reliability. Even if the RAS is not configured to shed load, it is necessary that the design and performance of RAS considers interactions with DERs, especially when penetration of DERs is high. As such, the RAS design and analysis should consider the impact of DERs. Consideration of the potential future impact of DERs on RAS design and performance may or may not need to be specifically addressed in a future revision of this Directory.

Directory # 8 - System Restoration

Applicable NERC Standards

- EOP-005- System Restoration from Blackstart Resources
- EOP-006- System Restoration Coordination
- PRC-005- Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance”

Determination of Impact from DER and VER:

As the deployment of DER continues, an item for consideration is if a determination should be made on which DER would be eligible as a Blackstart Resource to benefit system restoration to improve resilience. Although the general process for determining eligibility as a Blackstart Resource may address the need, the issue of limiting the ability of intermittent resources, such as solar resources, to provide restoration services needs to be considered. The standards under which certain DER were interconnected to the distribution system and the choice of inverter hardware may limit the usability of these facilities as black start resources. A revision to the Criteria to address if and how the use of intermittent resources in system restoration could contribute to reliability should be considered in a future revision.

Directory # 11 - Disturbance Monitoring Equipment Criteria

Applicable NERC Standards

- PRC-002- Disturbance Monitoring and Reporting Requirements

Determination of Impact from DER and VER:

The Directory focuses on event data for analysis that may be useful for model validation, in addition to disturbance monitoring equipment, sequence of events recorders, and fault recorders. For a system disturbance, it will be beneficial to record the response of larger DER installations or aggregations and assess whether DER will impact existing disturbance monitoring equipment. From a model validation perspective, the response of aggregate DERs may be adequate and further discussion when the Directory is revised should be considered.

Directory # 12 - Automatic UFLS Program Requirements (Scheduled to be retired in 2021)

NPCC’s Regional Standard, PRC-006-NPCC-2 has received full approval from all applicable governmental authorities within the NPCC Region.

Directory Prioritization Recommendation

DER and VER impact on NPCC's Reliability Directories should be considered during the next scheduled review with due consideration given to the suggested prioritization schedule below.

Directory #	Title	Last Task Force Review	Current Status	Next Scheduled Review	Task Force	Priority
1	Design and Operation of the Bulk Power System	September 2015	TFCP/TFCO Drafting Scope	2021	TFCP/TFCO	High
2	Emergency Operations	June 2018		2021	TFCO	Low
4	System Protection Criteria	January 2020		2023	TFSP	High to Moderate
5	Reserve	September 2019		2022	TFCO	Moderate
6	Reserve Sharing Groups	September 2019		2022	TFCO	Low
7	Remedial Action Schemes	December 2020		2023	TFCP/TFSP	Low
8	System Restoration	October 2017	TFCO CO-11 Begin Review 1st Qtr. 2021	2021	TFCO	Moderate
11	Disturbance Monitoring Equipment Criteria	October 2016	Currently Under Review TFSP Posting 1 st Qtr. 2021	2021	TFSP	Low
12	UFLS Program Requirements	July 2013	TFSS to Retire in 2021	N/A	TFSS	N/A

Appendix A- Future Directory Review Considerations

As Directories are reviewed there are some questions the Task Forces could use as they examine the Criteria for revision. The following questions were developed using some information from the NERC Energy Reliability Assessment Task Force (ERATF). They are only suggestions and not meant to be an all-encompassing set of issues to raise during the Directory reviews. The suggestions below may bridge operations and planning related Directory Criteria.

Directory Review Considerations:

1. What flexibility is required to balance volatility in resource and load uncertainty through multiple operating horizons and seasons of the year to achieve NPCC's reliability and energy sufficiency?
2. Should emergency procedures and reserve criteria be revised to reflect current and new fleet structure and operating needs?
3. When and how should demand response be considered when assessing fuel availability and energy adequacy?
4. Should the fuel availability / energy adequacy of battery or long-duration storage be evaluated and considered in NPCC's Directories?
5. Should NPCC's more specific Criteria consider including the reliability benefit of strategically overbuilding a similar technology (i.e., solar) augmented by either storage or some portion of the firm capacity fleet (albeit operating at low-capacity factors only when needed) could provide for a resilient and reliable transition?
6. Should longer time horizons be considered for long term planning studies with local decarbonization regulatory goals considered? (for example, Electric Vehicle charging on the distribution system and build out of the transmission system needed to accommodate and integrate offshore wind.)
7. How could large amounts of DER affect UFLS performance and System Protection functions. Do the Directories need to be revised to include additional more stringent or specific requirements for effective grounding, harmonics, short circuit etc., beyond what may be published in standards such as IEEE-1547-2018 and IEEE-519?
8. Are schedules for NPCC reviews unnecessarily time consuming and posing obstacles to the deployment of DER or VER? Examples are the time to examine and approve a Remedial Action Scheme or perform an A-10 analysis to determine if system elements are part of or newly recognized as part of the NPCC Bulk Power System.
9. Should NPCC have disturbance monitoring and performance measuring equipment and communication requirements for the Distribution System to capture data for system events?

Appendix B- Decarbonization Goals within NPCC

- CT- 80% below 2001 levels by 2050
- MA- Net zero by 2050 (ET) and 80% below 1990 by 2030
- ME- Net zero by 2050 (ET) and 80% below 1990 by 2030
- NH- 80% below 1990 levels by 2050
- NY- Net zero by 2040, 9,000 Offshore Wind, 6000 Solar, 3000 Storage
- RI- 80% below 1990 levels by 2050
- VT- 80% below 1990 levels by 2050
- NS- Net Zero by 2050
- ON- 30% below 2005 levels by 2030 (Paris Climate)
- QC-37.5 percent of 1990 levels by 2030, Net Zero by 2050
- US Federal Proposed goal-net-zero emissions no later than 2050

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization
2. **Number:** CIP-002-~~76~~
3. **Purpose:** To identify and categorize BES Cyber Systems (~~BCS~~) and their associated BES Cyber Assets (~~BCA~~) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~~~BCS~~ could have on the reliable operation of the BES. Identification and categorization of ~~BES Cyber Systems~~~~BCS~~ support appropriate protection against compromises that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (~~RAS~~) where the ~~Remedial Action Scheme~~~~RAS~~ is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the

starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:
All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-76:

4.2.3.1. Cyber Assets-systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets-systems associated with communication networks and data communication links between discrete Electronic Security Perimeters logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.2.4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.3.4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4.4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Date: See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-002-6.~~

6. Background: This standard provides “bright line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard. Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

The CIP Cyber Security Standards use the “BES Cyber System” term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware

~~protection to a grouping rather than individual Cyber Assets and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term “BES Cyber System” is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

Reliable Operation of the BES

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity’s responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

Real-time Operations

~~One characteristic of the BES Cyber Asset is a real time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than “Real time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

Categorization Criteria

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement R1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 — Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the CIP Cyber Security Standards.~~

~~Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

- ~~• **Electronic Access Control or Monitoring Systems (“EACMS”)** — Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~
- ~~• **Physical Access Control Systems (“PACS”)** — Examples include: authentication servers, card systems, and badge control systems.~~
- ~~• **Protected Cyber Assets (“PCA”)** — Examples include, to the extent they are within the ESP: file servers, FTP servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*
- i. Control Centers and backup Control Centers;
 - ii. Transmission stations and substations;
 - iii. Generation resources;
 - iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
 - v. ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System; and
 - vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.
- 1.1.** Identify each of the high impact ~~BES Cyber System~~BCS according to Attachment 1, Section 1, if any, at each asset;
- 1.2.** Identify each of the medium impact ~~BES Cyber System~~BCS according to Attachment 1, Section 2, if any, at each asset; and
- 1.3.** Identify each asset that contains a low impact ~~BES Cyber System~~BCS or SCI that hosts any portion of a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~BCS or SCI that hosts any portion of a low impact BCS is not required).
- 1.4.** Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).
- 1.5.** Identify associated SCI that hosts any portion of the medium impact ~~BES Cyber System~~BCS identified in Part 1.2 above or their associated EACMS, PACS or PCAs.
- M1.** Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, ~~and Parts 1.1, and 1.2, 1.4 and 1.5.~~
- R2.** Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- 2.1.** Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and
 - 2.2.** Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

- M2.** Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

- 1.1. Compliance Enforcement Authority:** “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.
- 1.2. Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
 - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
 - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.
- 1.3. Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.4. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Operations Planning	High	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~SystemsBCS, and associated SCI~~, five percent or fewer of identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, five or fewer identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category. OR	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and ~~BES Cyber SystemsBCS and associated SCI~~, more than five but less than or equal to 10 identified ~~BES Cyber~~	For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and ~~BES Cyber AssetsBCS and associated SCI~~, more than 10 but less than or equal to 15 identified ~~BES Cyber~~	~~SystemsBCS and associated SCI~~, more than 15 percent of identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber SystemsBCS and associated SCI~~, more than 15 identified ~~BES Cyber SystemsBCS or associated SCI~~ have not been categorized or have been incorrectly categorized at a lower category. OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, and <u>associated SCI</u>, five percent or fewer high or medium ~~BES Cyber Systems~~BCS or <u>associated SCI</u>, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, or <u>associated SCI</u>, five or fewer high or medium ~~BES Cyber Systems~~BCS or <u>associated SCI</u>, have not been identified.	~~Systems~~BCS or <u>associated SCI</u> have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and <u>associated SCI</u>, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS or <u>associated SCI</u> have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES~~	~~Assets~~BCS or <u>associated SCI</u> have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and <u>associated SCI</u>, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS or <u>associated SCI</u> have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES~~	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and <u>associated SCI</u>, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS or <u>associated SCI</u> have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS and <u>associated SCI</u>, more than 15 high or medium impact ~~BES Cyber Systems~~BCS or <u>associated SCI</u> have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~Cyber Systems~~ BCS and associated SCI, more than five but less than or equal to 10 high or medium ~~BES Cyber Systems~~ BCS or associated SCI have not been identified.	~~Cyber Systems~~ BCS and associated SCI, more than 10 but less than or equal to 15 high or medium ~~BES Cyber Systems~~ BCS or associated SCI have not been identified.	
R2.	Operations Planning	Lower	The Responsible Entity did not complete its review and update for the identification required for <u>Requirement R1</u> within 15 calendar months but less than or equal to 16 calendar months of the previous review. (<u>Requirement R2 Part R2.1</u>) OR The Responsible Entity did not complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for <u>Requirement R1</u> within 16 calendar months but less than or equal to 17 calendar months of the previous review. (<u>Requirement R2 Part R2.1</u>) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for <u>Requirement R1</u> within 17 calendar months but less than or equal to 18 calendar months of the previous review. (<u>Requirement R2 Part R2.1</u>) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for <u>Requirement R1</u> within 18 calendar months of the previous review. (<u>Requirement R2 Part R2.1</u>) OR The Responsible Entity failed to complete its approval of the identifications required by <u>Requirement R1</u> by the CIP Senior Manager or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002- ~~76~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>Requirement</u> R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (<u>Requirement R2 Part R2.2</u>)	<u>Requirement</u> R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (<u>Requirement R2 Part R2.2</u>)	<u>Requirement</u> R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (<u>Requirement R2 Part R2.2</u>)	delegate according to Requirement R2 within 18 calendar months of the previous approval. (<u>Requirement R2 Part R2.2</u>)

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan for CIP-002-~~76~~.”
- ~~See Appendix 1. The Interpretation in Appendix 1 was developed under a prior version of the Reliability Standard, CIP-002-5.1, and is being carried forward to subsequent versions.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating

Each ~~BES Cyber System~~BCS used by and located at any of the following:

- 1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
- 1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
- 1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
- 1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating

Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

- 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those each discrete~~ shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
- 2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are those shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.
- 2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

- 2.4.** Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
- 2.5.** Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

- 2.6.** Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 2.7.** Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 2.8.** Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.
- 2.9.** Each ~~Remedial Action Scheme (RAS)~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.
- 2.10.** Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

- 2.11.** Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.
- 2.12.** Each Control Center or backup Control Center, not included in the High Impact Rating, used to perform the reliability tasks of a Transmission Operator in real-time to monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a Line	Weight Value per Line
less than 100 kV (not applicable)	(not applicable)
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

- 2.13.** Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

- 3.1.** Control Centers and backup Control Centers.
- 3.2.** Transmission stations and substations.
- 3.3.** Generation resources.
- 3.4.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

- 3.5. ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System.
- 3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4—Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-6 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-6. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-6

CIP-002-6 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “...that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-6. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions

- ~~Balancing Load and Generation~~
- ~~Controlling Frequency (Real Power)~~
- ~~Controlling Voltage (Reactive Power)~~
- ~~Managing Constraints~~
- ~~Monitoring & Control~~
- ~~Restoration of BES~~
- ~~Situational Awareness~~
- ~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

Entity Registration	BC	BA	TDP	TD	DP	GDP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
 - ~~Providing actual reserve generation when called upon (GO, GOP)~~
 - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
 - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
 - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
 - ~~Zone protection for breaker failure (DP, TO, TOP)~~
 - ~~Breaker protection (DP, TO, TOP)~~
 - ~~Current, frequency, speed, phase (TO, TOP, GO, GOP)~~
- ~~Remedial Action Schemes~~
 - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
 - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
 - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- ~~Calculation of Area Control Error (ACE)~~
 - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
 - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
 - ~~Ability to identify load change need (BA)~~
 - ~~Ability to implement load changes (TOP, DP)~~
- ~~Manually Initiated Load shedding~~
 - ~~Ability to identify load change need (BA)~~
 - ~~Ability to implement load changes (TOP, DP)~~
- ~~Non spinning reserve (contingency reserve)~~

- Know generation status, capability, ramp rate, start time (GO, BA)
- Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
 - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
 - Software to calculate unit adjustments (BA)
 - Transmit adjustments to individual units (GOP)
 - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
 - Frequency source, schedule (BA)
 - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
 - Sensors, stator control system, feedback (GO)
- Capacitive resources
 - Status, control (manual or auto), feedback (TOP, TO, DP)
- Inductive resources (transformer tap changer, or inductors)
 - Status, control (manual or auto), feedback (TOP, TO, DP)
- Static VAR Compensators (SVC)
 - Status, computations, control (manual or auto), feedback (TOP, TO, DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)

- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

Monitoring and Control

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches
 - ~~SCADA (TOP, GOP)~~
 - ~~Substation automation (TOP)~~~~

Restoration of BES

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path
 - ~~Through black start units (TOP, GOP)~~
 - ~~Through tie lines (TOP, GOP)~~~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

Situational Awareness

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC, BA)~~
- ~~Change management (TOP, GOP, RC, BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

Inter-Entity Coordination

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and~~

operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- ~~Scheduled interchange (BA, TOP, GOP, RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

When the drafting team uses the term “Facilities,” there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as, “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-6, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may

~~be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~

~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~

~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

High Impact Rating

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

Medium Impact Rating

~~No additional evaluation is necessary for BES Cyber Systems that have already been identified as high impact.~~

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is “to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance.” In particular, it requires that “as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency.” The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a “long term” reliability planning, i.e. that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as “Reliability Must Run,” and this designation is distinct from those generation Facilities designated as “must run” for market stabilization purposes. Because the use of the term “must run” creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units

~~designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL 003, then BES Cyber Systems for that unit are categorized as medium impact.~~

~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~• Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.~~

~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~• Criterion 2.9 categorizes BES Cyber Systems for Remedial Action Schemes as medium impact. Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~
- ~~• Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~
- ~~• Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500-MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

Transmission

~~The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical~~

~~borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.~~

- ~~● Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~
- ~~● Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the “Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface.” This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

- ~~● Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~
 - ~~■ Excluded radial facilities that would only provide support for single generation facilities.~~
 - ~~■ Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

Additionally, in Attachment 1 of NERC's "Integrated Risk Assessment Approach—Refinement to Severity Risk Index" document, the report used an average MVA line loading based on kV rating:

- ~~230 kV → 700 MVA~~
- ~~345 kV → 1,300 MVA~~
- ~~500 kV → 2,000 MVA~~
- ~~765 kV → 3,000 MVA~~

In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~
- ~~Multiple point (or multiple tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

- ~~1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~

- ~~2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4.: there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~• Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC 014.2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.~~
- ~~• Criterion 2.7 is sourced from the NUC 001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC 001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~
- ~~• Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide-area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~
- ~~• Criterion 2.9 designates as medium impact those BES Cyber Systems for those Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~
- ~~• Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted~~

~~that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~In ERCOT, the Load acting as a Resource (“Laar”) Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~• Criterion 2.12 categorizes medium impact BES Cyber Systems associated with Control Centers and backup Control Centers, including associated data centers, that monitor and control BES Transmission Lines with an aggregate weighted value of 6000 or higher, and that have not already been included in Part 1. The drafting team included additional qualifications in this criterion that would ensure the required level of impact to the BES is defined and a risk threshold associated to establish a floor for applicable medium impact BES Cyber Systems.~~

~~The total aggregated weighted value is used to account for the impact to the BES. The 6000 aggregate weighted value threshold defined in criterion 2.12 provides a sufficient differentiation for medium and low impact BES Cyber Systems associated with Control Centers that monitor and control BES Transmission Lines. SDT analysis of Transmission Control Centers validated that those facilities that may have significant impact are categorized at an appropriate level commensurate with the associated risk.~~

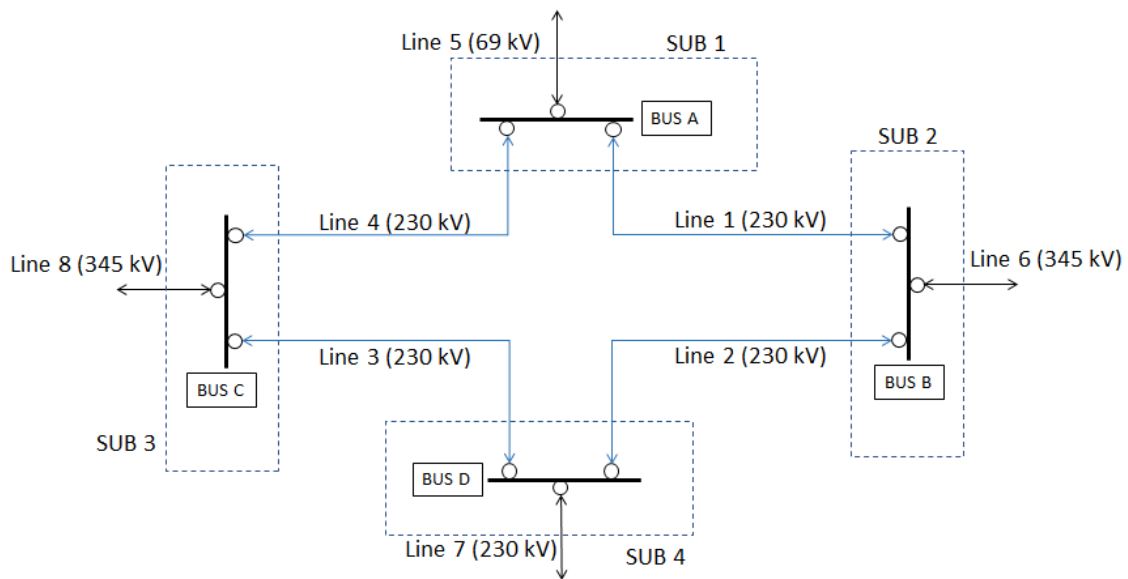
~~In the terms of applicable BES Transmission Lines, the following should be considered:~~

- ~~▪ All BES Transmission Lines that are energized at voltages between 100 kV and 499 kV and are monitored and controlled by a Control Center, including associated data center(s).~~

- All BES Transmission Lines, including those that connect to neighboring entities, that are monitored and controlled by the Responsible Entity's Control Center, including associated data center(s).
- Multiple point (or multiple tap) lines are considered to contribute a single weight value per line. For example, a single 230 kV multiple point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. For example, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.12 Examples:

In example 1 below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.



Example 1

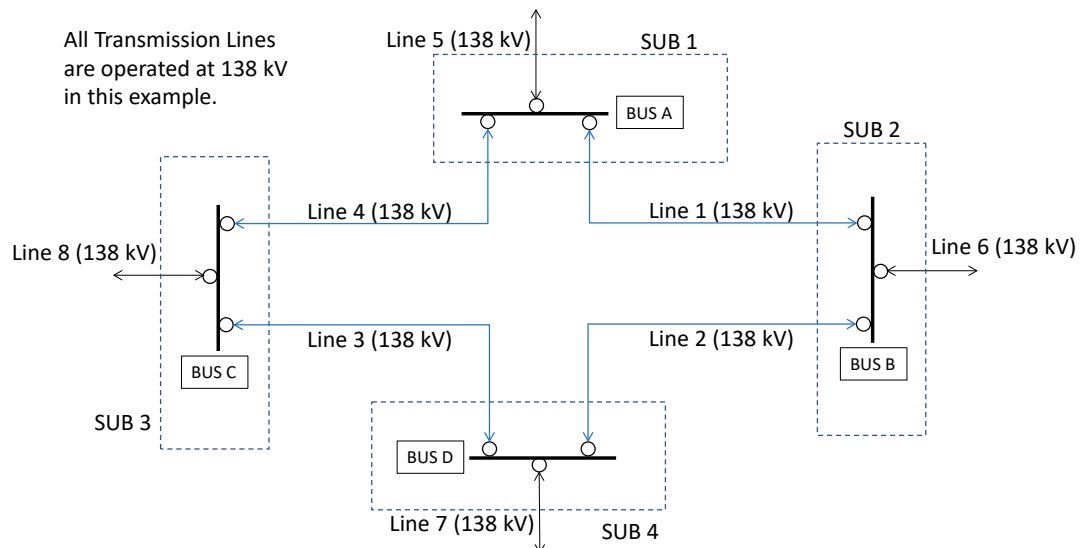
The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in Criterion 2.12. In accordance with Criterion 2.12, the BES Cyber System(s) associated with the Control Center should be categorized as medium impact BES Cyber System(s).

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
~~less than 100 kV~~ ~~(not applicable)~~	~~(not applicable)~~	~~Line 5~~	~~N/A~~
~~100 kV to 199 kV~~	~~250~~	~~None~~	~~0~~
~~200 kV to 299 kV~~	~~700~~	~~Line 1, Line 2, Line 3, Line 4, Line 7~~	~~3500~~
~~300 kV to 499 kV~~	~~1300~~	~~Line 6, Line 8~~	~~2600~~
~~500 kV and above~~	~~0~~	~~None~~	~~0~~

Calculation

$$700+700+700+700+700+1300+1300 = 6100$$

In the additional example below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.



Example 2

The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 2000, which is below the minimum threshold for a medium impact rating required in Criterion 2.12. The BES Cyber System(s) associated with the Control Center in this example should be categorized as a low impact BES Cyber System(s) pursuant to Criterion 3.1.

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
less than 100 kV (not applicable)	(not applicable)	None	N/A
100 kV to 199 kV	250	Line 1, Line 2, Line 3, Line 4, Line 5, Line 6, Line 7, Line 8	2000
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	None	0
500 kV and above	0	None	0

Calculation

$$250+250+250+250+250+250+250+250= 2000$$

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that “control” 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating

No additional evaluation is necessary for BES Cyber Systems that have already been identified as high or medium impact. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact. Note that low impact BES Cyber Systems do not require discrete identification, only identification of the asset containing the low impact BES Cyber System(s).

Restoration Facilities

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection~~

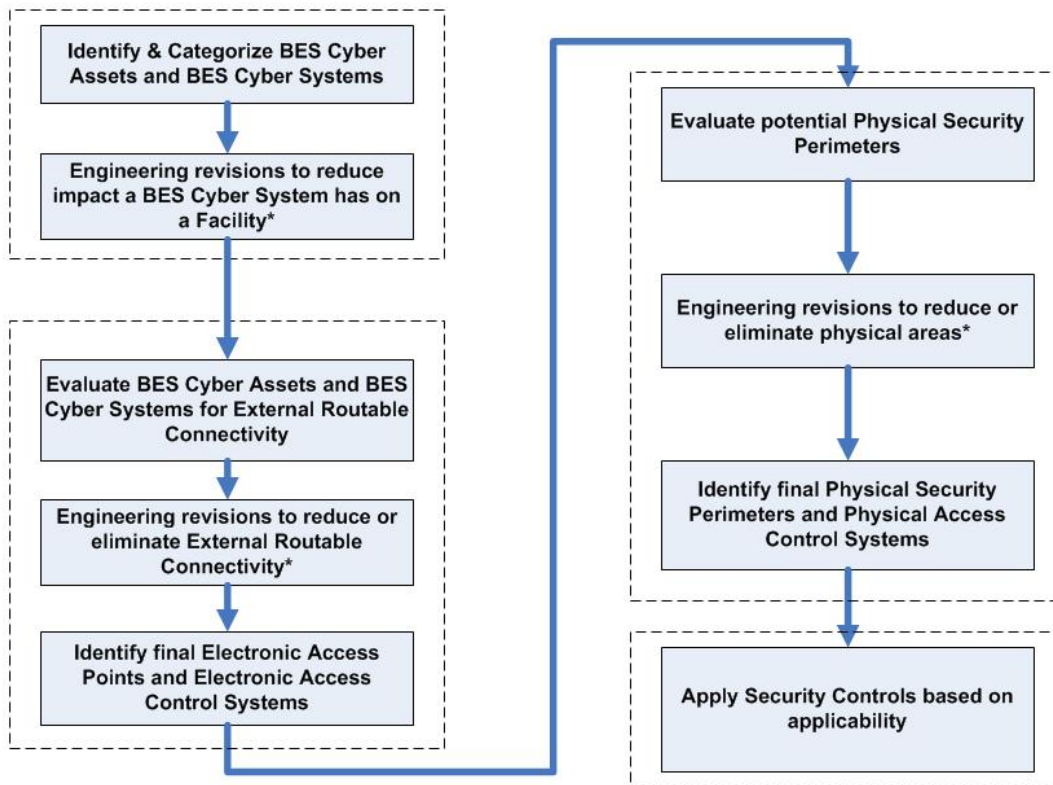
~~point of the generation unit(s) to be started, as identified in the Transmission Operator’s restoration plan, default to the category of low impact; however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator’s Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~

Overview (Generation Facility)



* - Engineering revisions will need to be reviewed for cost justification, operational safety requirements, support requirements, and technical limitations.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of “bright line” criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real time operation of the BES. The CIP Senior Manager’s approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

1

Requirement Number and Text of Requirement

CIP-002 5.1, Requirement R1

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

- i. Control Centers and backup Control Centers;
- ii. Transmission stations and substations;
- iii. Generation resources;
- iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

- ~~1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~

~~Attachment 1, Criterion 2.1~~

~~2. Medium Impact Rating (M)~~

~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~

- ~~2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

Questions

~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase “shared BES Cyber Systems.”~~

~~The Interpretation Drafting Team identified the following questions in the RFI:~~

- ~~1. Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~
- ~~2. Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~
- ~~3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

Responses

~~**Question 1: Whether the phrase “shared BES Cyber Systems,” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?**~~

~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states “Identify each of~~

~~the medium impact BES Cyber Systems according to Attachment 1, Section 2...~~ Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states ~~“Each BES Cyber System...associated with any of the following [criteria].”~~ (emphasis added)

~~Additionally, the Background section of CIP-002-5.1 states that “[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System.” The Background section also provides:~~

~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Question 2: Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~

~~The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.~~

~~The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~

~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.” For criterion 2.2: “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.~~

~~Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~The phrase applies to each discrete BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-~~98~~
3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. **Generator Operator**
 - 4.1.4. **Generator Owner**
 - 4.1.5. **Reliability Coordinator**
 - 4.1.6. **Transmission Operator**

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:
All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-98:

4.2.3.1. Cyber Assets-systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets-systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters (ESPs)~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.2.4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.4.2.3.4.~~ The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.4.2.3.5.~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project CIP-003-8~~

~~6. Background:~~

~~Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities’ management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.~~

~~The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term program may refer to the organization’s overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.~~

~~Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- 1.1.** For its high impact and medium impact ~~BES Cyber Systems~~BCS and associated SCI, if any:
 - 1.1.1.** Personnel and training (CIP-004);
 - 1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
 - 1.1.3.** Physical security of ~~BES Cyber Systems~~BCS (CIP-006);
 - 1.1.4.** System security management (CIP-007);
 - 1.1.5.** Incident reporting and response planning (CIP-008);
 - 1.1.6.** Recovery plans for ~~BES Cyber Systems~~BCS (CIP-009);
 - 1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
 - 1.1.8.** Information protection (CIP-011); and
 - 1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
 - 1.2.** For its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS and associated SCI, if any:
 - 1.2.1.** Cyber security awareness;
 - 1.2.2.** Physical security controls;
 - 1.2.3.** Electronic access controls;
 - 1.2.4.** Cyber Security Incident response;
 - 1.2.5.** Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and
 - 1.2.6.** Declaring and responding to CIP Exceptional Circumstances.
- M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.
- R2.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact ~~BES Cyber Systems~~BCS and their associated SCI that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact ~~BES Cyber Systems~~BCS or their associated SCI ~~BES Cyber Assets~~ is not required. Lists of authorized users are not required.

- M2.** Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.
- R3.** Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- M3.** An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.
- R4.** The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- M4.** An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.3. Compliance Monitoring and Assessment Processes:~~

- ~~• Compliance Audits~~
- ~~• Self-Certifications~~
- ~~• Spot-Checking~~
- ~~• Compliance Investigations~~
- ~~• Self-Reporting~~
- ~~• Complaints~~

~~1.4. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems BCS~~ and associated SCI but did not address one of the nine topics required by <u>Requirement R1. (Requirement R1 Part 1.1)</u> OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems BCS~~	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems BCS~~ and associated SCI but did not address two of the nine topics required by <u>Requirement R1. (Requirement R1 Part R1.1)</u> OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems BCS~~	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems BCS~~ and associated SCI but did not address three of the nine topics required by <u>Requirement R1. (Requirement R1 Part R1.1)</u> OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems BCS~~ and associated SCI as required by <u>Requirement</u>	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems BCS~~ and associated SCI but did not address four or more of the nine topics required by <u>Requirement R1. (Requirement R1 Part R1.1)</u> OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems BCS~~ and associated SCI as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>and associated SCI</u> as required by <u>Requirement R1</u> within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ <u>BCS and associated SCI</u> as required by <u>Requirement R1</u> by the CIP Senior	<u>and associated SCI</u> as required by <u>Requirement R1</u> within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems <u>BCS and associated SCI</u> as required by <u>Requirement R1</u> by the CIP Senior	R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ <u>BCS and associated SCI</u> as required by <u>Requirement R1</u> by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (<u>Requirement R1</u>)	required by <u>Requirement R1</u>. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by <u>Requirement R1</u> within 18 calendar months of the previous review. (<u>Requirement R1</u>) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but did not address one of the six topics required by <u>Requirement R1</u>. (<u>Requirement R1 Part 1.2</u>)	Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but did not address two of the six topics required by <u>Requirement R1</u>. (<u>Requirement R1 Part 1.2</u>)	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~, but did not address three of the six topics required by <u>Requirement R1</u>. (<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ as required by <u>Requirement R1</u> within 17 calendar	medium impact ~~BES Cyber Systems BCS and associated SCI~~ as required by <u>Requirement R1</u> by the CIP Senior Manager within 18 calendar months of the previous approval. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but did not address four or more of the six topics required by <u>Requirement R1</u>.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES~~ <u>Cyber Systems BCS and associated SCI</u> as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not complete its	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES~~ <u>Cyber Systems BCS and associated SCI</u> as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not complete its	months but did complete this review in less than or equal to 18 calendar months of the previous review. (<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval.	(<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems BCS and associated SCI~~ as required by Requirement R1. (<u>Requirement R1 Part 1.2</u>) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES-Cyber Systems BCS~~ and associated SCI as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (<u>Requirement R1 Part R1.2</u>)	approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES-Cyber Systems BCS~~ and associated SCI as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (<u>Requirement R1 Part R1.2</u>)	(<u>Requirement R1 Part R1.2</u>)	in CIP-002 containing low impact ~~BES-Cyber Systems BCS~~ and associated SCI as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (<u>Requirement R1 Part R1.2</u>)
R2	Operations Planning	Lower	The Responsible Entity documented its cyber security plan(s) for its assets containing low	The Responsible Entity documented its cyber security plan(s) for its assets containing low	The Responsible Entity documented the physical access controls for its assets containing low impact ~~BES-Cyber~~	The Responsible Entity failed to document and implement one or more cyber security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact ~~BES Cyber Systems BCS and associated SCI~~ but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (<u>Requirement R2</u>) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (<u>Requirement R2</u>) OR The Responsible Entity documented	impact ~~BES Cyber Systems BCS and associated SCI~~ but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (<u>Requirement R2</u>) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but failed to document physical security controls according to Requirement R2, Attachment 1,	~~Systems BCS and associated SCI~~ but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (<u>Requirement R2</u>) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact ~~BES Cyber Systems BCS and associated SCI~~ but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (<u>Requirement R2</u>) OR	plan(s) for its assets containing low impact ~~BES Cyber Systems BCS and associated SCI~~ according to Requirement R2, Attachment 1. (<u>Requirement R2</u>)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS~~ and <u>associated SCI</u> but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS~~ and <u>associated SCI</u>	Section 2. (<u>Requirement</u> R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS~~ and <u>associated SCI</u> but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (<u>Requirement</u> R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all	The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems BCS~~ and <u>associated SCI</u> but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to manage its <u>TCA</u> according to Requirement R2, Attachment 1, Section 5.1. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u>, but failed to	Dial-up Connectivity that provides access to low impact ~~BES~~ <u>Cyber System(s)</u> <u>BCS</u>, per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (<u>Requirement</u> R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES~~ <u>Cyber Systems</u> <u>BCS</u> and associated <u>SCL</u>, but failed to include the process for identification, classification, and response to Cyber Security Incidents	Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to implement mitigation for the introduction of malicious code for <u>TCA</u> managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (<u>Requirement R2</u>)	according to Requirement R2, Attachment 1, Section 4. (<u>Requirement R2</u>) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES-Cyber Systems~~ <u>BCS</u> and <u>associated SCI</u> but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to	the introduction of malicious code for <u>TCA</u> managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (<u>Requirement R2</u>) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES-Cyber System-BCS~~ according to Requirement R2, Attachment 1, Section 5.3. (<u>Requirement R2</u>)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to document mitigation for the introduction of malicious code for <u>TCA</u> managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				document mitigation for the introduction of malicious code for <u>TCA</u> managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (<u>Requirement</u> R2) OR The Responsible Entity documented its plan(s) for <u>TCA</u> and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (<u>Requirement</u> R2)		
R3	Operations Planning	Medium	The Responsible Entity has identified	The Responsible Entity has identified	The Responsible Entity has identified by name a	The Responsible Entity has not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	Operations Planning	Lower	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-98)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (Requirement R4)	change in less than 50 calendar days of the change. (Requirement R4)	change. (Requirement R4)	OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ [See "Project 2016-02 Virtualization Implementation Plan."](#)

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact ~~BES-Cyber Systems~~ BCS.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	

Version	Date	Action	Change Tracking
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
<u>9</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact ~~BES-Cyber Systems~~BCS or their associated SCI

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact ~~BES-Cyber Systems~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES-Cyber Systems~~BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES-Cyber Systems~~BCS within the asset, (2) the asset or the locations of the SCI hosting low impact BES Cyber Assets within the asset, and (3) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact ~~BES-Cyber System(s)~~BCS or its associated SCI identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

- 3.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:
 - i. between a low impact ~~BES-Cyber System(s)~~BCS and a ~~Cyber Asset(s)~~system(s) outside the asset containing low impact ~~BES-Cyber System(s)~~BCS;
 - ii. between SCI hosting a low impact BCS and a system(s) outside the asset(s) containing the SCI hosting a low impact BCS;
 - iii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES-Cyber System(s)~~BCS or their associated SCI; and
 - iv. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).
- 3.2** Authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES-Cyber System(s)~~BCS or their associated SCI, per Cyber Asset or VCA capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

- 4.1 Identification, classification, and response to Cyber Security Incidents;
- 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;
- 4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
- 4.4 Incident handling for Cyber Security Incidents;
- 4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and
- 4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems BCS or its associated SCI~~, through the use of Transient Cyber Assets TCA or Removable Media. The plan(s) shall include:

- 5.1 For Transient Cyber Asset(s) TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset TCA capability):
 - Antivirus software, including manual or managed updates of signatures or patterns;
 - Application whitelisting; or
 - Other method(s) to mitigate the introduction of malicious code.
- 5.2 For Transient Cyber Asset(s) TCA managed by a party other than the Responsible Entity, if any:
 - 5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset TCA to a low impact ~~BES Cyber System BCS or its associated SCI~~ (per Transient Cyber Asset TCA capability):
 - Review of antivirus update level;

- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~BCS or its associated SCI; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS or its associated SCI.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact ~~BES-Cyber Systems~~BCS or their associated SCI

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
 - a. The asset, if any, or the locations of the low impact ~~BES-Cyber Systems~~BCS or their associated SCI within the asset; and
 - b. The Cyber Asset(s) VCA, or SCI specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact ~~BES-Cyber Systems~~BCS, routable communication between a low impact ~~BES-Cyber System(s)~~BCS and ~~a Cyber Asset(s)~~ systems outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact ~~BES-Cyber System(s)~~BCS and ~~a Cyber Asset(s)~~ systems outside the asset containing low impact ~~BES-Cyber System(s)~~BCS or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset~~TCA~~ and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Section 4—Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements. Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings. Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations

~~although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.~~

~~For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:~~

~~1.1.1 Personnel and training (CIP-004)~~

~~Organization position on acceptable background investigations~~

~~Identification of possible disciplinary action for violating this policy~~

~~Account management~~

~~Electronic Security Perimeters (CIP-005) including Interactive Remote Access~~

~~Organization stance on use of wireless networks~~

~~Identification of acceptable authentication methods~~

~~Identification of trusted and untrusted resources~~

~~Monitoring and logging of ingress and egress at Electronic Access Points~~

~~Maintaining up-to-date anti-malware software before initiating Interactive Remote Access~~

~~Maintaining up-to-date patch levels for operating systems and applications used to initiate~~

~~Interactive Remote Access~~

~~Disabling VPN "split tunneling" or "dual-homed" workstations before initiating Interactive~~

~~Remote Access~~

~~For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls~~

~~Physical security of BES Cyber Systems (CIP-006)~~

~~Strategy for protecting Cyber Assets from unauthorized physical access~~

~~Acceptable physical access control methods~~

~~Monitoring and logging of physical ingress~~

~~System security management (CIP-007)~~

~~Strategies for system hardening~~

~~Acceptable methods of authentication and access control~~

~~Password policies including length, complexity, enforcement, prevention of brute force attempts~~

~~Monitoring and logging of BES Cyber Systems~~

~~Incident reporting and response planning (CIP-008)~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

~~1.1.6 Recovery plans for BES Cyber Systems (CIP-009)~~

~~Availability of spare components~~

~~Availability of system backups~~

~~1.1.7 Configuration change management and vulnerability assessments (CIP-010)~~

~~Initiation of change requests~~

~~Approval of changes~~

~~Break-fix processes~~

~~1.1.8 Information protection (CIP-011)~~

~~Information access control methods~~

~~Notification of unauthorized information disclosure~~

~~Information access on a need-to-know basis~~

~~1.1.9 _____ Declaring and responding to CIP Exceptional Circumstances~~

~~Processes to invoke special procedures in the event of a CIP Exceptional Circumstance~~

~~Processes to allow for exceptions to policy that do not violate CIP requirements~~

~~For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:~~

~~1.2.1 _____ Cyber security awareness~~

~~Method(s) for delivery of security awareness~~

~~Identification of groups to receive cyber security awareness~~

~~1.2.2 _____ Physical security controls~~

~~Acceptable approach(es) for selection of physical security control(s)~~

~~1.2.3 _____ Electronic access controls~~

~~Acceptable approach(es) for selection of electronic access control(s)~~

~~1.2.4 _____ Cyber Security Incident response~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

~~1.2.5 _____ Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Acceptable use of Transient Cyber Asset(s) and Removable Media~~

~~Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media~~

~~Method(s) to request Transient Cyber Asset and Removable Media~~

~~1.2.6 _____ Declaring and responding to CIP Exceptional Circumstances~~

~~Process(es) to declare a CIP Exceptional Circumstance~~

~~Process(es) to respond to a declared CIP Exceptional Circumstance~~

~~Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.~~

~~In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

Requirement R2:

~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate “how” the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below:

Requirement R2, Attachment 1, Section 1—Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or “If you see something, say something” campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2—Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with

~~locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.~~

~~The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.~~

~~Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.~~

~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

Requirement R2, Attachment 1, Section 3—Electronic Access Controls

~~Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.~~

~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).~~

~~When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.~~

~~In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.~~

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR 61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles

away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

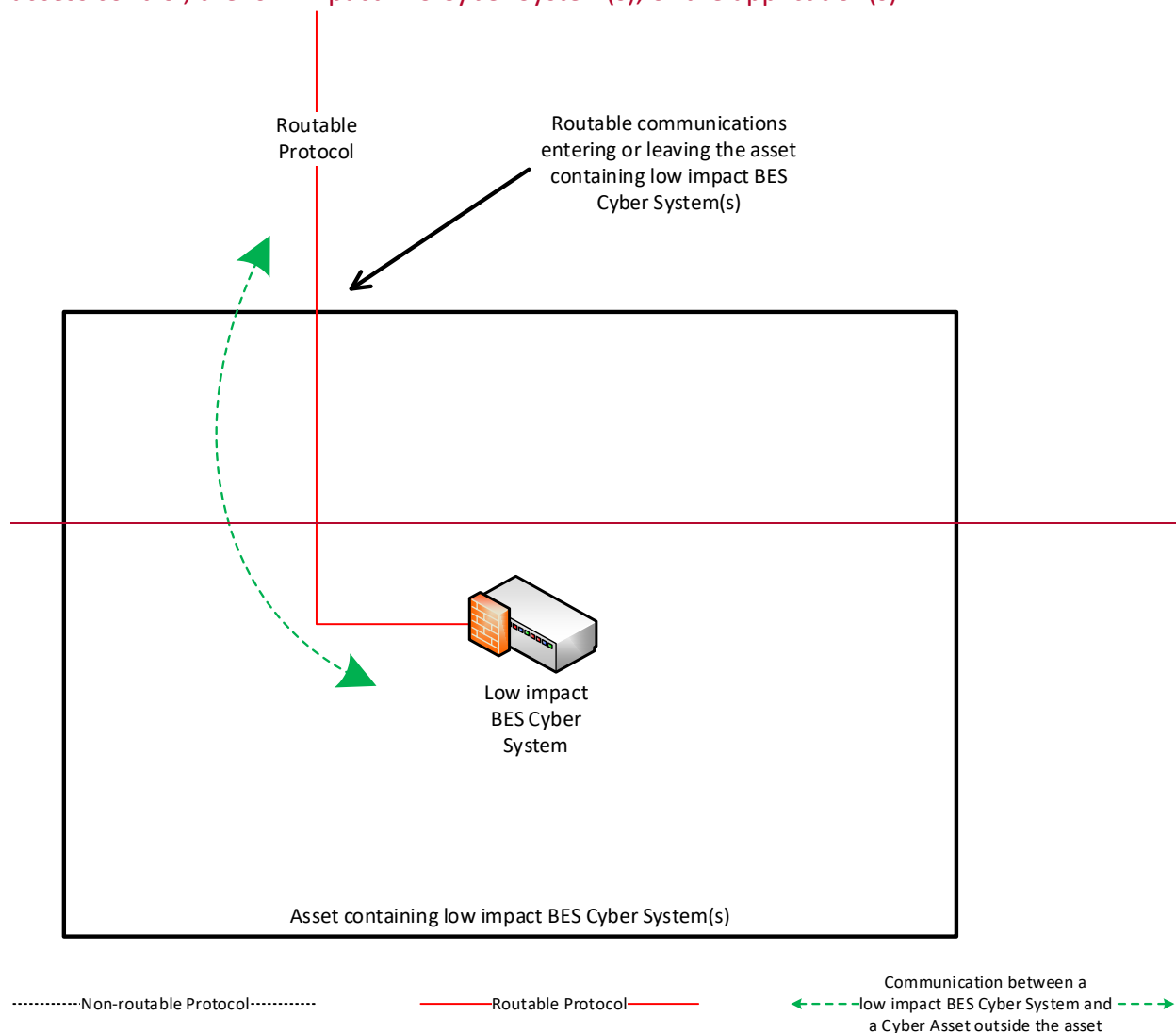
NOTE:

This is not an exhaustive list of applicable concepts.

The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

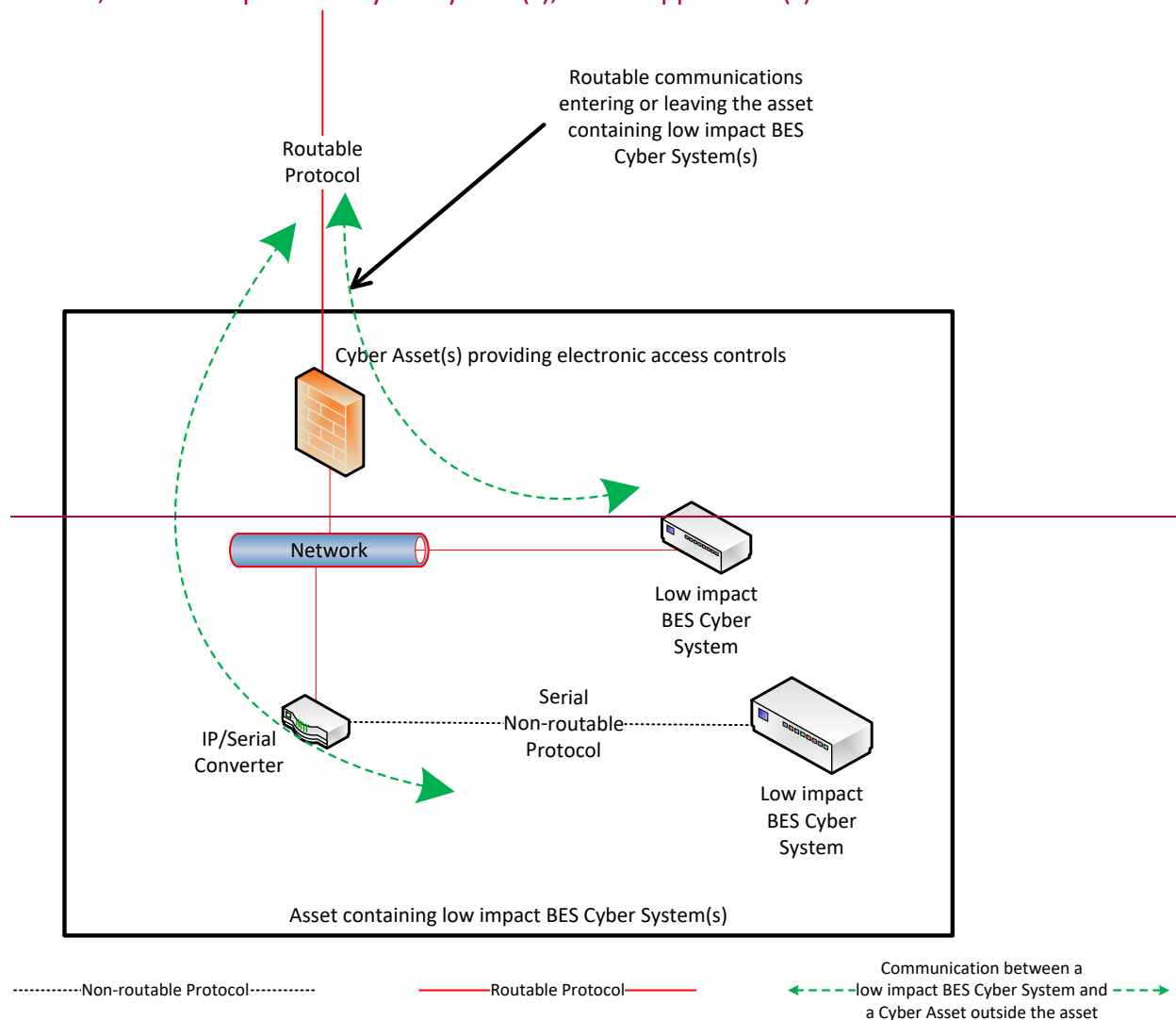
Reference Model 1—Host-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).

**Reference Model 1**

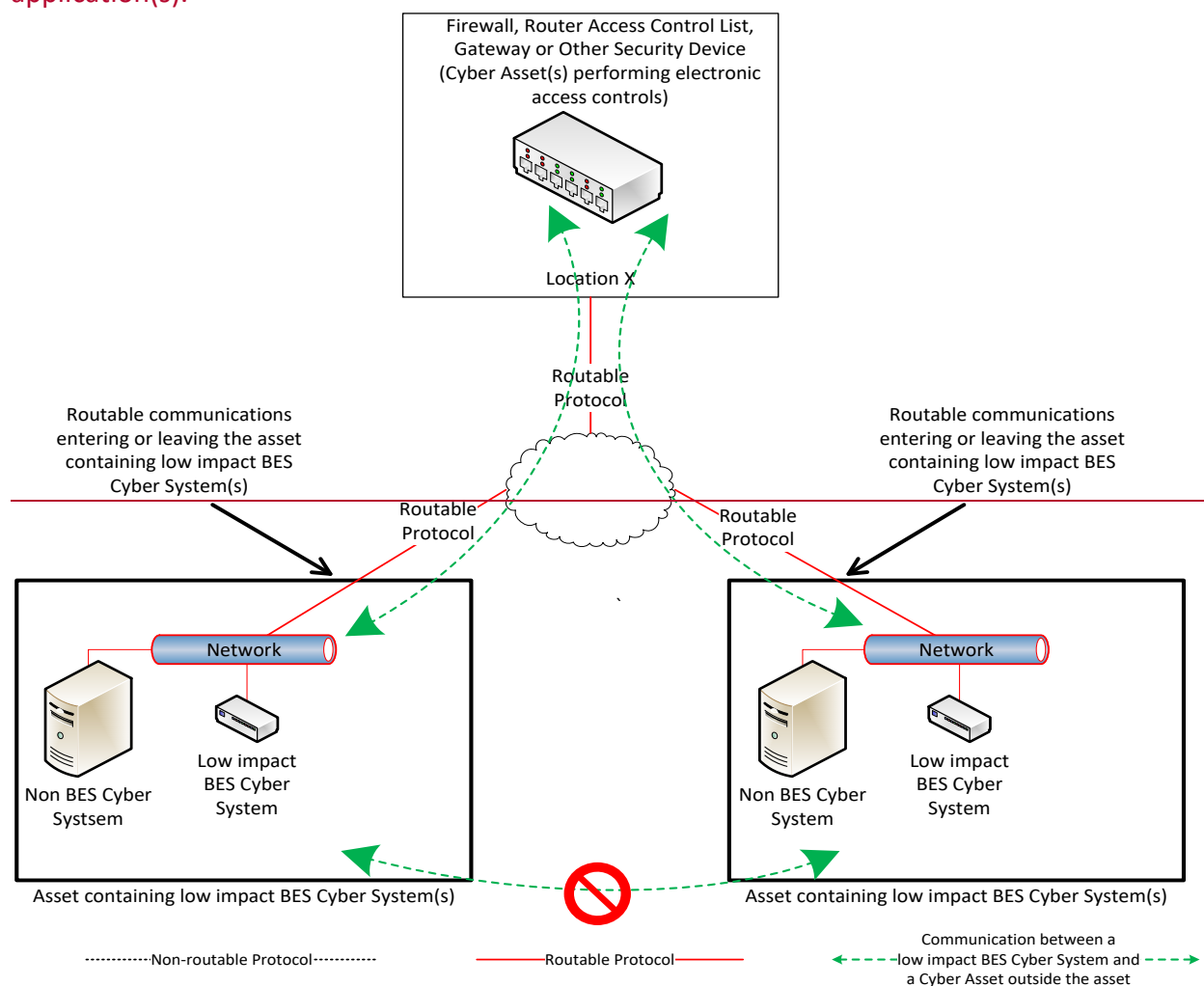
Reference Model 2—Network-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).

**Reference Model 2**

Reference Model 3—Centralized Network-based Inbound & Outbound Access Permissions

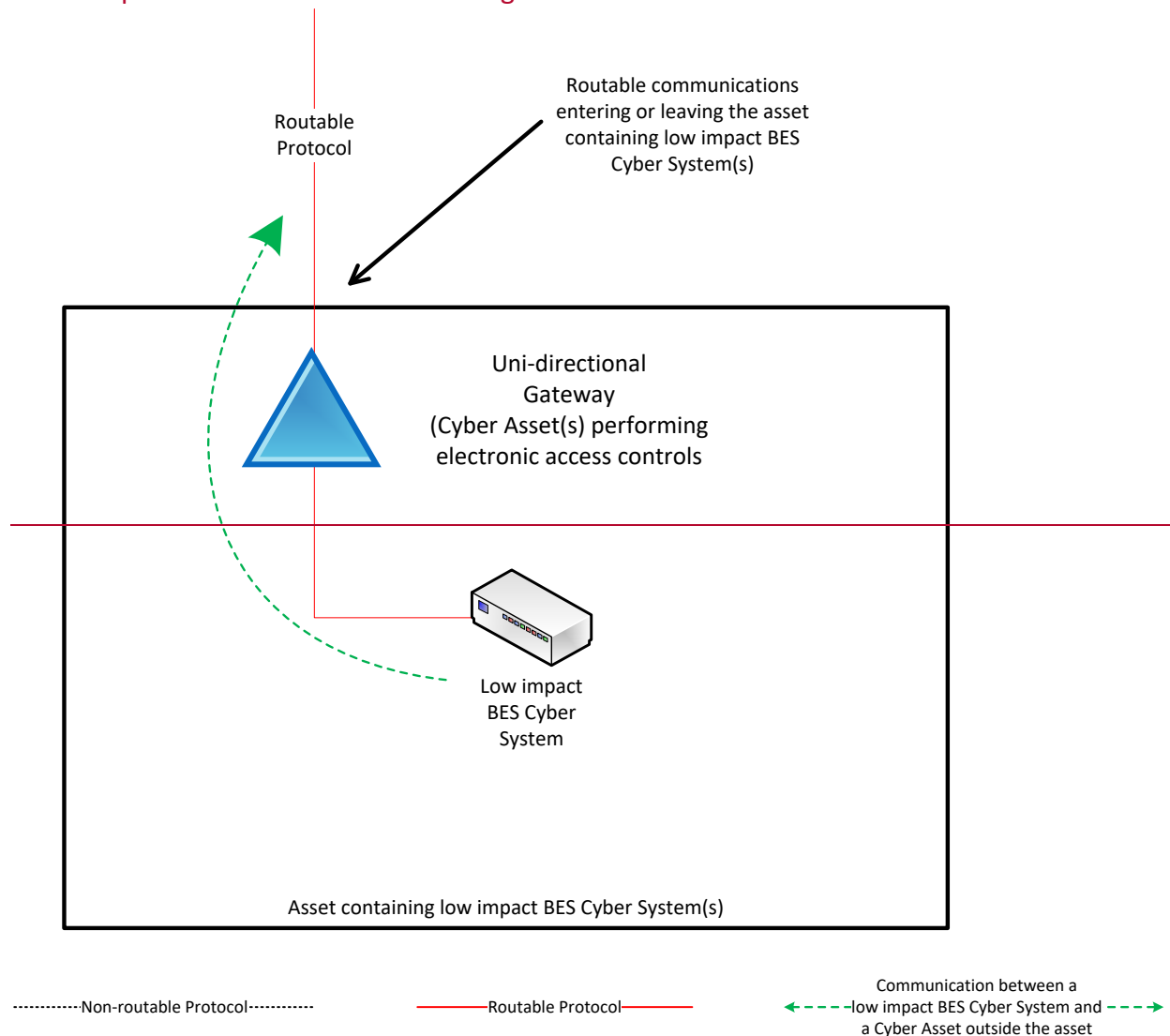
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at “Location X” to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4—Uni-directional Gateway

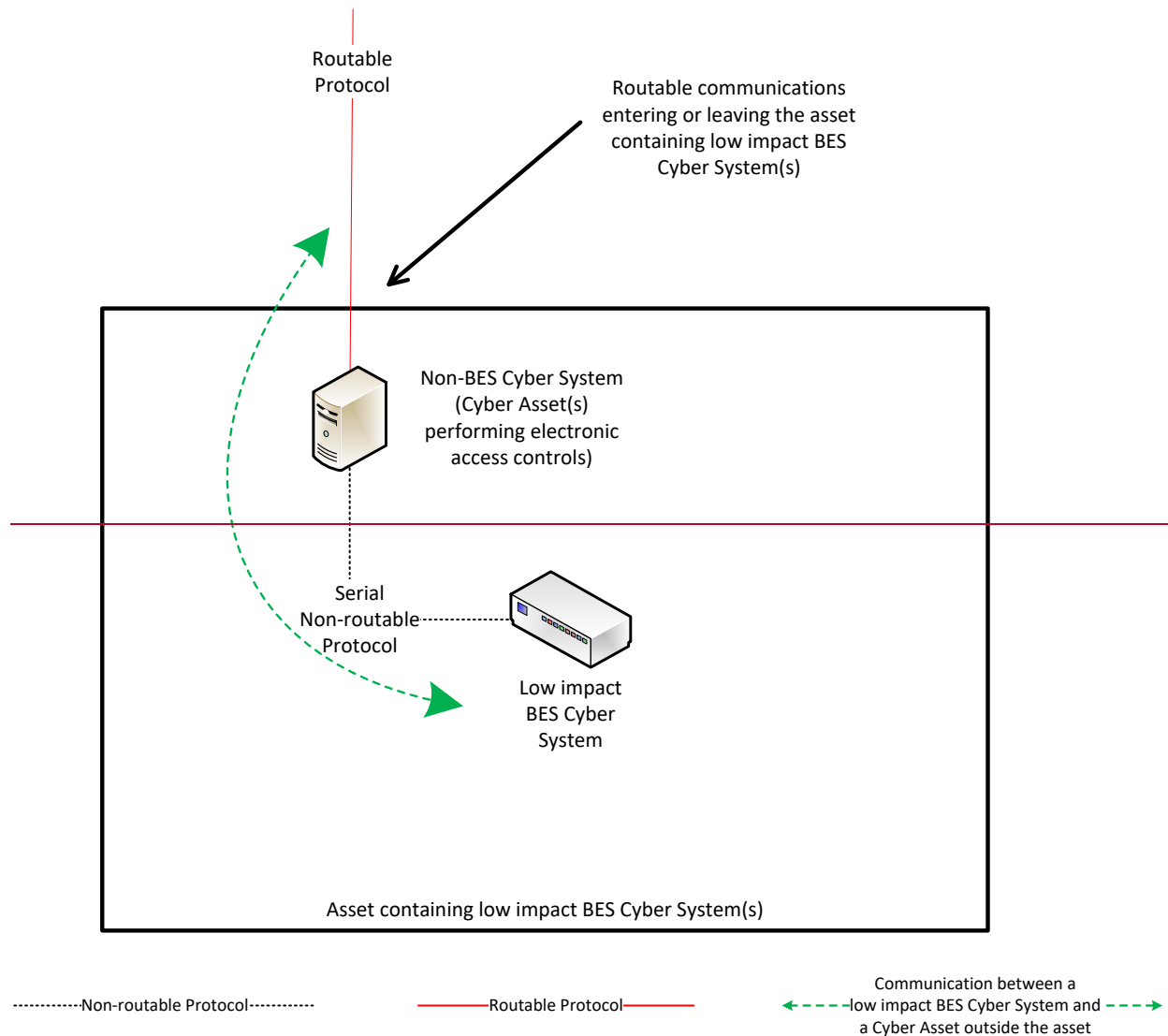
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way” (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5—User Authentication

This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user initiated interactive access.



Reference Model 5

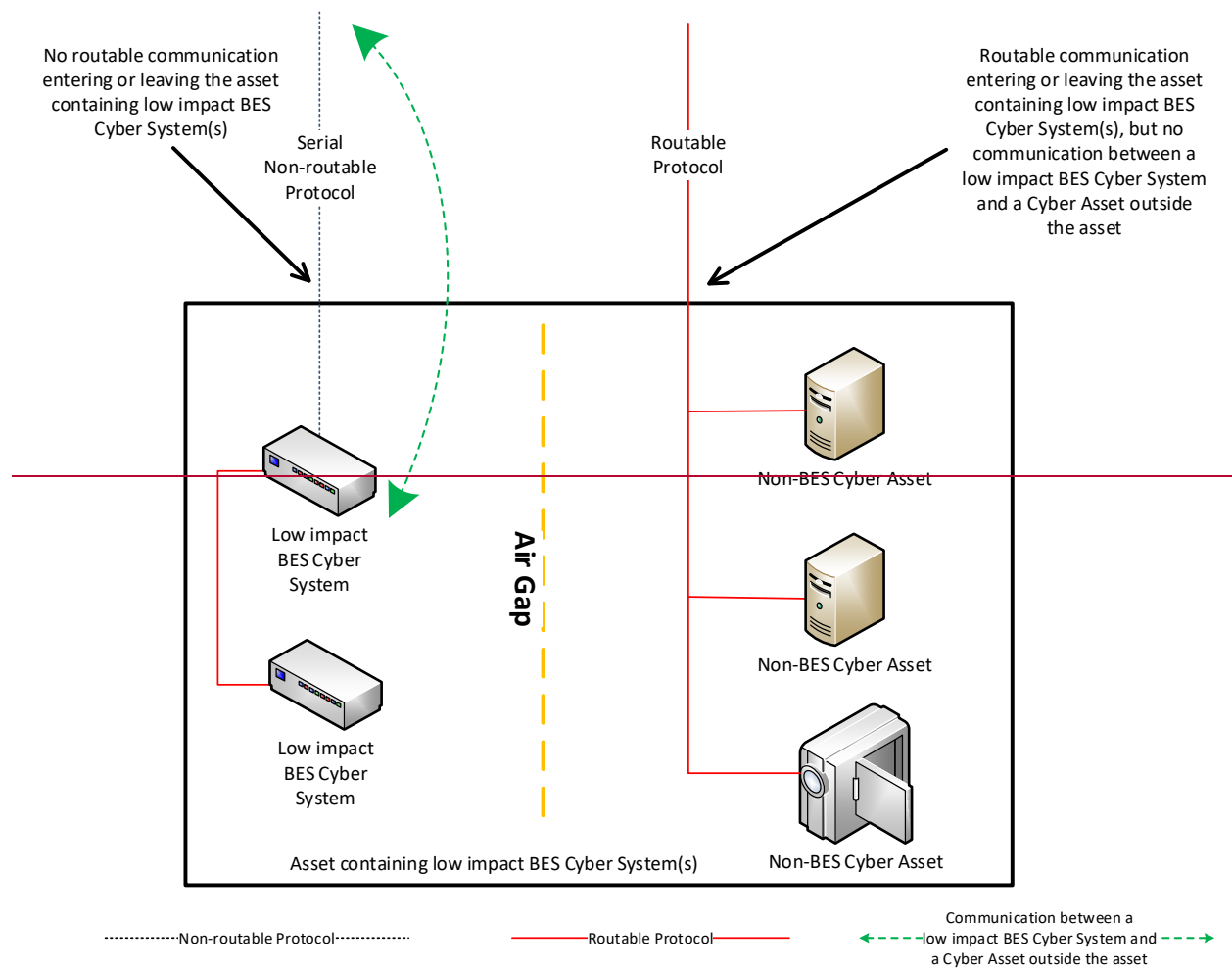
**Reference Model 8—Physical Isolation and Serial Non-routable Communications—
No Electronic Access Controls Required**

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;

The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.

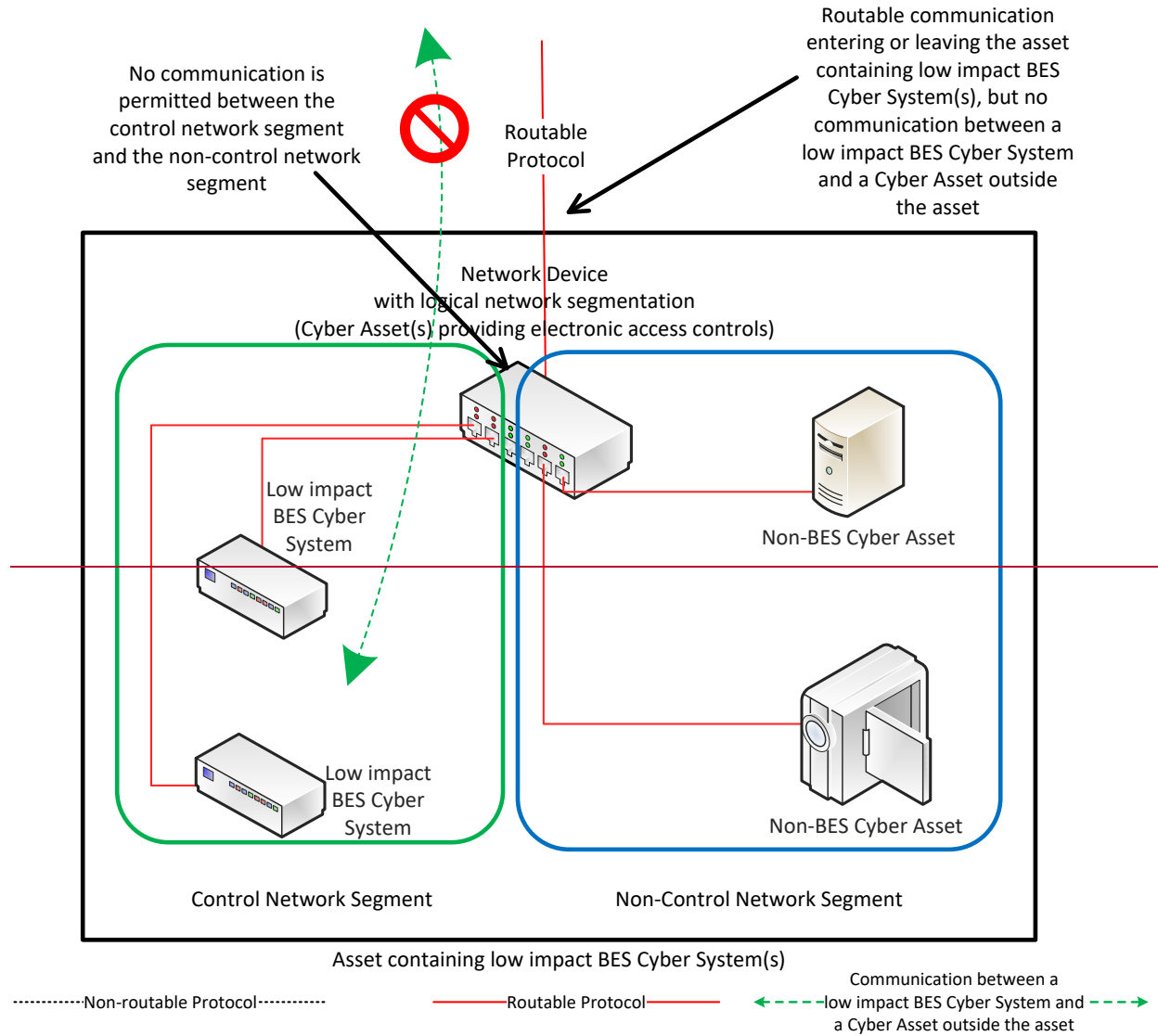
The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9—Logical Isolation—No Electronic Access Controls Required

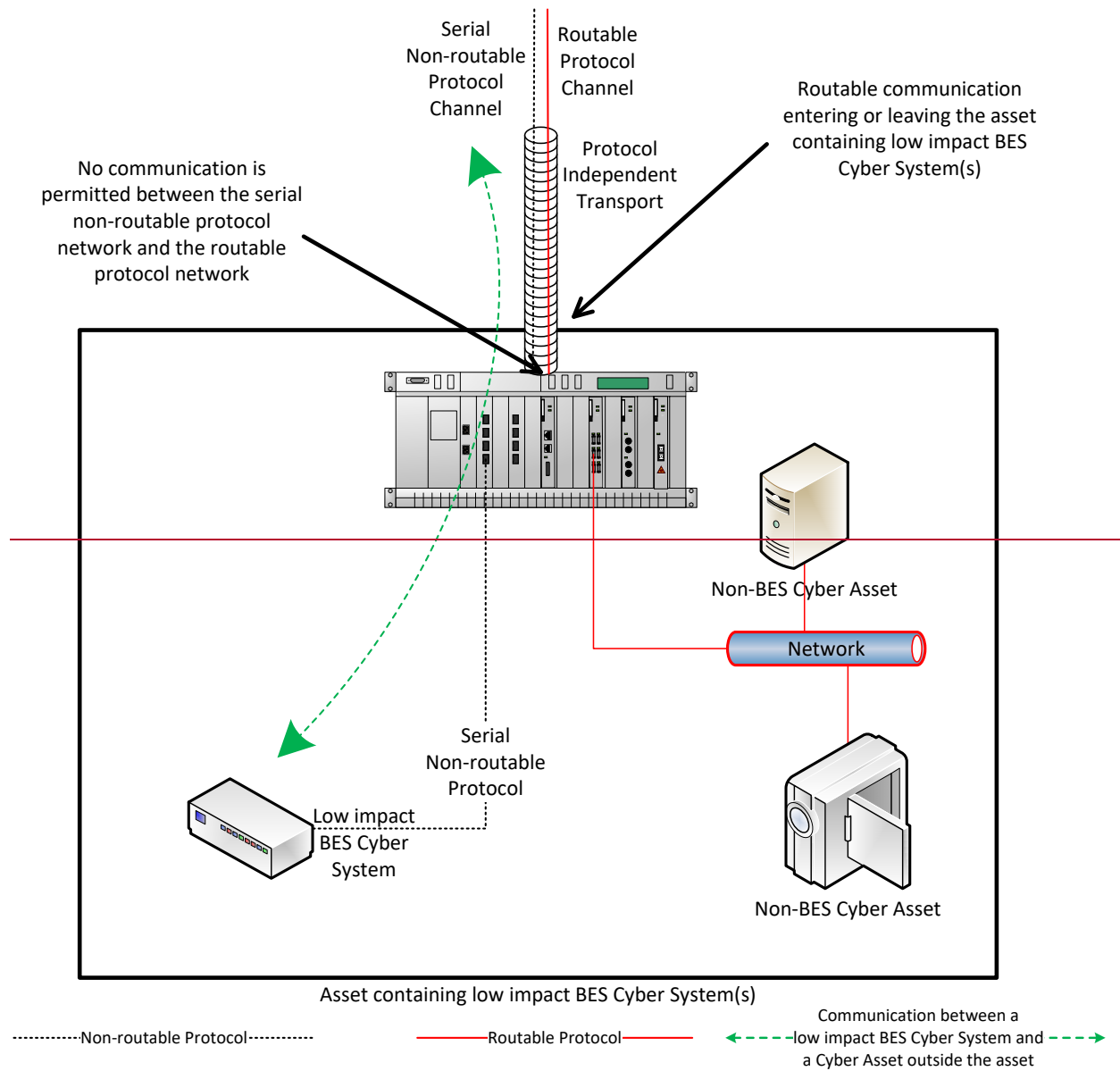
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10—Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network—No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide area network using a protocol independent transport that may carry routable and non-routable communication such as a Time Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.

A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

Dual homing or multiple network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4—Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5—Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

~~Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets can be one of many types of devices from a specially designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets.~~

~~Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~Examples of these temporarily connected devices include, but are not limited to:~~

~~Diagnostic test equipment;~~

~~Equipment used for BES Cyber System maintenance; or~~

~~Equipment used for BES Cyber System configuration.~~

~~To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.~~

~~With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.~~

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1—Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: ~~Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.~~

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code:

~~Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.~~

~~Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System. When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code. If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Requirement R2, Attachment 1, Section 5.2—Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party’s security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of “prior to connecting the Transient Cyber Assets” is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.⁴ Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back-up recovery may be part of the other party’s support. Entities may consider the “General Cybersecurity Procurement Language” and “The Supplier’s Life Cycle Security Program” when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

⁴ <http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014>

~~**Section 5.2.1:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~

~~Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.~~

~~Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.~~

~~Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.~~

~~Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.~~

~~**Section 5.2.2:** The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.~~

Requirement R2, Attachment 1, Section 5.3—Removable Media

~~Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.~~

~~**Section 5.3:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in~~

conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

Rationale for Requirement R1:

~~One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.~~

~~Annual review and approval of the cyber security policies ensures that the policies are kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

Rationale for Requirement R2:

~~In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.~~

~~Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.~~

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "...the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6...to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition...within one year of the effective date of this Final Rule."~~

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): “not used for time sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR 61850-90-5 R-GOOSE)”.

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to “the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.” The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to “...provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability.” Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference. FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for

~~responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.~~

~~Rationale for Requirement R4:~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-~~7~~ ~~6~~
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems ~~(BCS)~~ by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting ~~BES Cyber Systems~~ BCS.

4. Applicability:

- 4.1. Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

- 4.1.2. Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

- 4.1.2.1.** Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

- 4.1.2.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- 4.1.2.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

- 4.1.2.2.** Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

- 4.1.2.3.** Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

- 4.1.2.4.** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~4.1.5. Interchange Coordinator or Interchange Authority~~

~~4.1.6.~~ 4.1.5. Reliability Coordinator

~~4.1.7.4.1.6.~~ **Transmission Operator**

~~4.1.8.4.1.7.~~ **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

- 4.2.1.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- 4.2.1.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~76~~:

4.2.3.1. Cyber ~~Assets systems~~ at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets systems~~ associated with communication ~~networks and data communication links between discrete Electronic Security Perimeters logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).~~

~~4.2.3.2.4.2.3.3.~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.4.2.3.4.~~ The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.4.2.3.5.~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.6.~~ Responsible Entities that identify that they have no ~~BES-Cyber-Systems~~BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates: See “Project 2016-02 Virtualization” implementation Plan.~~” for CIP-004-6~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-~~76~~ Table R1 – Security Awareness Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-004-~~76~~ Table R1 – Security Awareness Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004- ~~76~~ Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated SCI Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated SCI	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~ <u>BCS or SCI</u> .	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

- R2.** Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-~~76~~ Table R2 – *Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- M2.** Evidence must include the training program that includes each of the applicable requirement parts in CIP-004-~~76~~ Table R2 – *Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-76 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. <u>Electronic Access Control or Monitoring System (EACMS)</u>; and 2. <u>Physical Access Control Systems (PACS)</u> Medium Impact ~~BES Cyber Systems~~ <u>BCS</u>, with External Routable Connectivity <u>(ERC) or Interactive Remote Access (IRA)</u>, and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI, with ERC or IRA, hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information <u>(BCSI)</u> and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for ~~BES Cyber Systems~~ <u>BCS and SCI</u>; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~ <u>BCS and SCI's</u> electronic interconnectivity and interoperability with other Cyber Assets <u>and VCA</u>, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-76 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with ~~External Routable Connectivity~~ <u>ERC or IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, <u>VCA or SCI</u>, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

CIP-004-76 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with ~~External Routable Connectivity~~ <u>ERC or IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

- R3.** Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~ BCS or their associated SCI that collectively include each of the applicable requirement parts in CIP-004-~~76~~ Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M3.** Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in CIP-004-~~76~~ Table R3 – Personnel Risk Assessment Program and additional evidence to demonstrate implementation of the program(s).

CIP-004-76 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-76 Table R3 — Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with <u>External Routable Connectivity</u> <u>ERC</u> or <u>IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven-year immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven-year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven-year criminal history records check.

CIP-004-76 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.3	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with ~~External Routable Connectivity~~ <u>ERC or IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

CIP-004-76 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.4	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> with ~~External Routable Connectivity~~ <u>ERC or Interactive Remote Access</u> <u>IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-76 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.5	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC- or ~~Interactive Remote Access~~ IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, <u>except during CIP Exceptional Circumstances, according</u> to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

- R4.** Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-~~76~~ Table R4 – Access Management Program. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*.
- M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in CIP-004-~~76~~ Table R4 – Access Management Program and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-76 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for ~~BES Cyber System~~ <u>Information</u>BCSI.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for ~~BES Cyber System~~ <u>Information</u>BCSI.

CIP-004-76 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated -documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-76 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-76 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Verify at least once every 15 calendar months that access to the designated storage locations for ~~BES Cyber System Information~~BCSI, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for ~~BES Cyber System Information~~BCSI; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

- R5.** Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-76 Table R5 – Access Revocation*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-76 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-76 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~<u>BCS</u> with ~~External Routable Connectivity~~<u>ERC</u> or ~~Interactive Remote Access~~<u>IRA</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated EACMS or PACS.</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated EACMS or PACS.</u>	A process to initiate removal of an individual's ability for unescorted physical access and ~~Interactive Remote Access~~<u>IRA</u> upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-76 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-76 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u> <u>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	For termination actions, revoke the individual's access to the designated storage locations for ~~BES Cyber System Information~~BCSI, whether physical or electronic (unless already revoked according to Requirement R5 <u>Part 5.1</u>), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing ~~BES Cyber System Information~~BCSI associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-76 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: EACMS <u>SCI hosting High Impact BCS or their associated EACMS.</u>	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any ~~individual applicable BES Cyber Assets~~systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.5	High Impact ~~BES Cyber Systems~~BCS and their associated: EACMS <u>SCI hosting High Impact BCS or their associated EACMS.</u>	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: - Workflow or sign-off form showing password reset within 30 calendar days of the termination; - Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or - Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.3. Compliance Monitoring and Assessment Processes:~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot-Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

~~2. Table of Compliance Elements~~**Violation Severity Levels**

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Requirement R1 Part 1.1)
R2	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1)	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2 Part R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)	training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)	Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)			
R3	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals.	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	unescorted physical access but did not confirm identity for two individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	(Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for	or more individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	3.2.1 and 3.2.2 for one individual. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not	electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	three individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)			
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where ~~BES Cyber System~~

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its ~~BES Cyberapplicable~~ <u>SS</u>systems, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.3</u>) OR The Responsible Entity has implemented processes to verify	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its ~~BES Cyberapplicable~~ <u>SS</u>systems, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.3</u>) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System InformationBCSI~~ is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than	groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~BES Cyberapplicable~~ <u>SS</u>systems, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.3</u>) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System InformationBCSI~~ is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~BES Cyber System InformationBCSI~~ storage locations, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.4</u>)	~~InformationBCSI~~ is located. (<u>Requirement R4 Part 4.1</u>) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (<u>Requirement R4 Part 4.2</u>) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~BES Cyberapplicable~~ <u>SS</u>systems, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.3</u>) OR

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	that access to the designated storage locations for ~~BES Cyber System Information~~ BCSI is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its ~~BES Cyber System Information~~ BCSI storage locations, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.4</u>)	(or equal to) 10% of its ~~BES Cyber System Information~~ BCSI storage locations, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.4</u>)		The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System Information~~ BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~BES Cyber System Information~~ BCSI storage locations, privileges were incorrect or unnecessary. (<u>Requirement R4 Part 4.4</u>)
R5	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for ~~BES Cyber System~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~ IRA upon a termination action or complete the removal within	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~ IRA upon a termination action or complete the removal within 24 hours of the termination action but did not	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or ~~BES Cyber System Information~~ BCSI storage locations. (<u>Requirement R5 Part R5</u>) OR

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Information BCSI~~, but for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (Requirement R5 Part 5.4)	24 hours of the termination action but did not initiate those removals for one individual. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more	initiate those removals for two individuals. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for ~~BES Cyber System~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access IRA~~ upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2)

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (<u>Requirement R5 Part 5.5</u>) OR The Responsible Entity has implemented one or more process(es) to determine and document	process(es) to revoke the individual's access to the designated storage locations for ~~BES-Cyber-System~~ ~~InformationBCSI~~ but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (<u>Requirement R5 Part 5.3</u>)	~~InformationBCSI~~ but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (<u>Requirement R5 Part 5.3</u>)	

R #	Violation Severity Levels (CIP-004-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Requirement R5 Part 5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents~~None.~~ See “Project 2016-02 Virtualization Implementation Plan.”**Version History**

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact ~~BES Cyber Systems~~ <u>BCS</u> .
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — ~~Electronic Security Perimeter(s)~~BES Cyber System -Logical Isolation
2. **Number:** CIP-005-~~87~~
3. **Purpose:** To ~~manage electronic access to protect~~ BES Cyber Systems (BCS) against ~~compromise by permitting only known and controlled communication to and from the system and logically isolating all other communication by specifying a controlled~~ Electronic Security Perimeter to reduce the likelihood of misoperations or instability in the BES. in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~87~~:

- 4.2.3.1. Cyber ~~Assets-systems~~ at Facilities regulated by the Canadian Nuclear Safety Commission.
- 4.2.3.2. Cyber ~~Assets-systems~~ associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).
- 4.2.3.3. ~~Cyber Ssystems associated with communication links between Cyber Assets, or Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.~~
- 4.2.3.3.4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.4.4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
- 4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~ BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

- 5. **Effective Date:** See Project 2016-02 Virtualization Implementation Plan, ~~for Project 2019-03.~~

~~**Background:** Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its~~

~~documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described:

High Impact BES Cyber Systems — Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

High Impact BES Cyber Systems with Dial-up Connectivity — Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

High Impact BES Cyber Systems with External Routable Connectivity — Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

Medium Impact BES Cyber Systems — Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

Medium Impact BES Cyber Systems at Control Centers — Only applies to medium impact BES Cyber Systems located at a Control Center.

Medium Impact BES Cyber Systems with Dial-up Connectivity — Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.

Medium Impact BES Cyber Systems with External Routable Connectivity — Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

Protected Cyber Assets (PCA) — Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Electronic Access Points (EAP) — Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Physical Access Control Systems (PACS) — Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Electronic Access Control or Monitoring Systems (EACMS) — Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-~~87~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-005-~~87~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: ~~1.~~ Protected Cyber Asset (PCA); ~~1-2.~~ Physical Access Control Systems (PACS) hosted on SCI; and ~~2-3.~~ Electronic Access Control or Monitoring System (EACMS) hosted on SCI Medium Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: ~~1.~~ PCA; ~~1-2.~~ PACS hosted on SCI; and ~~2-3.~~ EACMS hosted on SCI	~~All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP~~ ~~Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).~~	~~An e~~Examples of evidence may include, but is not limited to, ~~a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP~~documentation that includes the configuration of systems ~~that enforce electronic access control and logical isolation and document business need~~ such as: • ~~Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment);~~ • ~~SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration);-~~ ~~that enforces electronic access control and logical isolation and documents the business need.~~

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~ Logical Isolation			
Part	Applicable Systems	Requirements	Measures
1.2	<u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>PCA;</u> <u>PACS; or</u> <u>EACMS</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> <u>PCA;</u> <u>PACS; or</u> <u>EACMS</u> <u>EACMS that perform logical isolation for a High Impact BCS</u> <u>EACMS that perform logical isolation for a Medium Impact BCS</u> <u>High Impact BES Cyber Systems with External Routable Connectivity and their associated:</u> PCA <u>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</u> PCA	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~ <u>Implement for applicable systems as follows:</u> <u>1.2.1. Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability.</u> <u>1.2.2. Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications.</u> <u>1.2.3. Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.</u>	~~An e~~<u>Examples</u> of evidence may include, but is not limited to, ~~network diagrams showing all external routable communication paths and the identified EAPs~~<u>documentation that includes the configuration of systems that enforce access control and logical isolation such as:</u> <u>Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment)</u> <u>Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems</u> <u>SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).</u>

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~ Logical Isolation			
Part	Applicable Systems	Requirements	Measures
1.3	<u>High Impact BCS and their associated:</u> <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>Medium Impact BCS connected to a network via routable protocol and their associated:</u> <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated:</u> <u>• PCA;</u> <u>• PACS; or</u> <u>• EACMS</u> ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	<u>Protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of:</u> <u>• confidentiality and integrity controls (such as encryption), or</u> <u>• Physical controls that restrict access to the cabling and other nonprogrammable communication components,</u> <u>excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).</u> ~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of e~~Evidence may include, but is not limited to, <u>architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption)</u>~~a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~

CIP-005- ~~87~~ Table R1 – ~~Electronic Security Perimeter~~ Logical Isolation			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>4-3. EACMS hosted on SCI</u> Medium Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>SCI with Dial-up Connectivity hosting High or Medium Impact BCS or their associated:</u> • <u>PCS;</u> • <u>PACS; or</u> • <u>EACMS</u>	~~Where technically feasible, p~~Perform authentication when establishing Dial-up Connectivity with applicable ~~Cyber Assets~~systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-~~87~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.5	<u>High Impact BCS and their associated:</u> <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>Medium Impact BCS at Control Centers and their associated:</u> <u>1. PCA;</u> <u>2. PACS hosted on SCI; and</u> <u>3. EACMS hosted on SCI</u> <u>SCI at Control Centers hosting High or Medium Impact BCS or their associated:</u> <u>• PCA;</u> <u>• PACS, or</u> <u>• EACMS</u> ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	~~Have one or more methods for~~ Detecting known or suspected malicious <u>Internet Protocol (IP)</u> communications ~~for both inbound and outbound communications~~<u>entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.</u>	An example of evidence may include, but is not limited to, documentation that malicious <u>Internet Protocol (IP)</u> communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

- R2.** For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the ~~Each~~ Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in CIP-005-~~87~~ Table R2 –Remote Access Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M2.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in CIP-005-~~87~~ Table R2 –Remote Access Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-87 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~Interactive Remote Access (IRA) and their associated: • <u>PCA</u> <u>SCI with IRA hosting High or Medium Impact BCS or their associated:</u> • <u>PCA;</u> • <u>PACS; or</u> • <u>EACMS;</u> <u>Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PCA;</u> • <u>PACS; or</u> • <u>EACMS</u>	<u>Ensure that authorized IRA is through an Intermediate System.</u> ~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams, ~~or~~ architecture documents, <u>or Management Systems reports that show all IRA is through an Intermediate System.</u>
2.2	<u>Intermediate Systems used to access applicable systems of Part 2.1</u>	<u>Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.</u>	An example of evidence may include, but is not limited to, architecture documents detailing where ~~encryption~~<u>confidentiality and</u>

CIP-005-~~87~~ Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
	~~High Impact BES Cyber Systems and their associated:~~ ~~1. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~	<u>integrity controls</u> initiates and terminates.
2.3	<u>Intermediate Systems used to access applicable systems of Part 2.1</u> ~~High Impact BES Cyber Systems and their associated:~~ ~~2. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~3. PCA~~	Require multi-factor authentication ~~for all Interactive Remote Access sessions~~<u>to the Intermediate System.</u>	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-87 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.4	High Impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with vendor remote access ~~External Routable Connectivity~~ and their associated: • PCA <u>SCI with vendor remote access hosting High or Medium Impact BCS or their associated:</u> • <u>PCA</u> <u>Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PCA</u>	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-~~87~~ Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.5	High Impact ~~BES Cyber Systems~~BCS <u>with vendor remote access</u> and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with <u>vendor remote access</u>~~External Routable Connectivity~~ and their associated: • <u>PCA</u> <u>SCI with vendor remote access hosting High or Medium Impact BCS or their associated:</u> • <u>PCA</u> <u>Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PCA</u>	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access IRA~~ and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the method(s) used to disable active vendor remote access (including ~~Interactive Remote Access IRA~~ and system-to-system remote access.), ~~such as: Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~

CIP-005-87 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
<u>2.6</u>	<u>Intermediate Systems used to access applicable systems of Part 2.1</u>	<u>Implement for applicable systems as follows:</u> <u>2.6.1.</u> <u>Restrict Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI.</u> <u>2.6.2.</u> <u>Permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.</u>	<u>Examples of evidence may include, but is not limited to, documentation that includes the following:</u> • <u>Configuration showing that the CPU and memory can only be shared with other IS.</u> • <u>Configuration showing how communications are controlled between the IS and applicable systems.</u>

- R3.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-005-~~7-8~~ Table R3 –Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M3.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in CIP-005-~~7-8~~ Table R3 – Vendor Remote Access Management for EACMS and PACS and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005- ~~87~~ Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~ BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~ BCS with External Routable Connectivity (ERC) <u>SCI hosting EACMS or PACS associated with High or Medium impact BCS</u> <u>Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS</u>	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~ BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~ BCS with External Routable	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include

CIP-005-~~87~~ Table R3 – Vendor Remote Access Management for EACMS and PACS

Part	Applicable Systems	Requirements	Measures
	~~Connectivity~~ ERC <u>SCI hosting EACMS or PACS associated with High or Medium impact BCS</u> <u>Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS</u>		terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting <u>known or suspected</u> malicious Internet Protocol (IP) communications <u>entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2</u> ~~for both inbound and outbound communications.~~ ~~(1.5)~~	The Responsible Entity did not document one or more processes for <u>CIP-005-~~78~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation</u>. (<u>Requirement R1</u>) OR The Responsible Entity did not <u>permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications.</u> ~~have all applicable Cyber Assetssystems connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP).~~ <u>protected by logical isolation</u> (<u>Requirement R1 Part 1.1</u>) OR <u>The Responsible Entity did not protectimplement, for</u>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability the Management Systems or Management Interfaces or applicable systems per Requirement R1, Part 1.2 External Routable Connectivity through the ESP was not through an identified EAP. (Requirement R1 Part 1.2.1)</u> <u>OR</u> <u>The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating</u>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>all other communications.</u> <u>(Requirement R1 Part 1.2.2)</u> <u>OR</u> <u>The Responsible Entity did</u> <u>not implement, for</u> <u>applicable systems, a</u> <u>method for denying</u> <u>communications from BCS</u> <u>and their associated PCAs to</u> <u>the Management Interfaces</u> <u>and Management Systems,</u> <u>per system capability</u> <u>(Requirement R1 Part 1.2.3)</u> <u>OR</u> <u>The Responsible Entity did</u> <u>not implement a method to</u> <u>protect the data traversing</u> <u>communication links, where</u> <u>the logical isolation spans</u> <u>multiple Physical Security</u> <u>Perimeters, through the use</u> <u>of confidentiality and</u> <u>integrity controls (such as</u> <u>encryption); or physical</u> <u>controls that restrict access</u> <u>to the cabling and other</u>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~nonprogrammable communication components protect confidentiality and integrity of the data traversing communications links per Requirement R1, Part 1.3.~~ The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing ~~D~~ ial-up ~~e~~ Connectivity with the applicable ~~Cyber Assets~~ systems, where technically feasible. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3;	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3;

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement Parts 2.1 through 2.3.		OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (<u>Requirement R2 Part 2.4</u>); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (<u>Requirement R2 Part 2.5</u>).	OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (<u>Requirement R2 Part 2.4</u>) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (<u>Requirement R2 Part 2.5</u>). OR <u>The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per</u>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>system capability</u> <u>(Requirement R2 Part 2.6.1)</u> OR <u>The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).</u>
R3.	The Responsible Entity did not document one or more processes for CIP-005- ~~87~~ Table R3 – Vendor Remote Access Management for EACMS and PACS. <u>(Requirement R3)</u>	The Responsible Entity had method(s) as required by Part 3.1 for EACMS <u>and SCI</u> <u>and -Management Modules of SCI</u> but did not have a method to determine authenticated vendor-initiated remote connections for PACS <u>(Requirement R3 Part 3.1)</u> . OR The Responsible Entity had method(s) as required by	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. <u>(Requirement R3)</u> OR The Responsible Entity had method(s) as required by Part 3.1 for PACS <u>and SCI</u> <u>and Management Modules of SCI</u> but did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for CIP-005- ~~78~~ Table R3 – Vendor Remote Access Management for EACMS and PACS. <u>(Requirement R3)</u> OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 <u>(Requirement R3)</u> .

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Part 3.2 for EACMS, ~~and SCI~~ <u>and Management Modules of SCI</u> but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (<u>Requirement R3 Part 3.2</u>).	connections for EACMS (<u>Requirement R3 Part 3.1</u>). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS, ~~and SCI~~ <u>and Management Modules of SCI</u> but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (<u>Requirement R3 Part 3.2</u>). <u>OR</u> <u>The Responsible Entity had method(s) as required by Part 3.1 for PACS and ~~and~~ EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of SCI (Requirement R3 Part 3.1).</u>	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>OR</u> <u>The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).</u>	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.” for Project 2019-03
- CIP-005-~~87~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
<u>8</u>	<u>TBD</u>	<u>Virtualization modifications and ERC/IRA</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems
2. **Number:** CIP-006-~~76~~
3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems ~~(BCS)~~ against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**

4.1.4 Generator Owner~~**4.1.5 Interchange Coordinator or Interchange Authority**~~~~**4.1.64.1.5 Reliability Coordinator**~~~~**4.1.74.1.6 Transmission Operator**~~~~**4.1.84.1.7 Transmission Owner**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:
All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-~~76~~:

4.2.3.1 Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.3.2~~ Cyber ~~Assets-systems~~ associated with communication ~~networks~~ and data communication links ~~between discrete Electronic Security Perimeters~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~4.2.3.24.2.3.3~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.34.2.3.4~~ The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.44.2.3.5~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.54.2.3.6~~ Responsible Entities that identify that they have no ~~BES Cyber Systems~~ BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan”

6. Background:

~~Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described:

High Impact BES Cyber Systems — Applies to BES Cyber Systems categorized as high impact according to the CIP-002 5.1 identification and categorization processes.

~~**Medium Impact BES Cyber Systems**—Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems without External Routable Connectivity**—Only applies to medium impact BES Cyber Systems without External Routable Connectivity.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity**—Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)**—Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)**—Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Protected Cyber Assets (PCA)**—Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Locally mounted hardware or devices at the Physical Security Perimeter**—Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-~~76~~ Table R1 – *Physical Security Plan*. [*Violation Risk Factor: Medium*] [*Time Horizon: Long Term Planning and Same Day Operations*].
- M1.** Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-~~76~~ Table R1 – *Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-~~76~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> without External Routable Connectivity (<u>ERC</u>) <u>SCI without ERC hosting Medium Impact BCS</u> Physical Access Control Systems (PACS) associated with: • High Impact <u>BCS</u> ~~BES Cyber Systems, or~~ • <u>Medium Impact ~~BES Cyber Systems~~ BCS with External Routable Connectivity</u> <u>ERC</u> • <u>SCI hosting High Impact BCS or their associated EACMS or PCA; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> <u>SCI hosting PACS associated with High Impact BCS</u> <u>SCI hosting PACS associated with Medium Impact BCS with ERC</u>	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-76 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.2	Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	~~Where technically feasible, u~~ Utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, <u>per system capability</u> .	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.5	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident ~~R~~esponse ~~P~~lan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.6	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS, or • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • <u>SCI hosting High Impact BCS or their associated EACMS or PCA; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> <u>SCI hosting PACS associated with High Impact BCS</u> <u>SCI hosting PACS associated with Medium Impact BCS with ERC</u>	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-76 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.7	Physical Access Control Systems (PACS) associated with: - High Impact ~~BES Cyber Systems~~BCS, or - Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC <u>SCI hosting High Impact BCS or their associated EACMS or PCAs; or</u> <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> <u>SCI hosting PACS associated with High Impact BCS</u> <u>SCI hosting PACS associated with Medium Impact BCS with ERC</u>	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident ~~R~~ <u>r</u> esponse ~~P~~ <u>p</u> lan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-~~76~~ Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.8	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~<u>BCS</u> with ~~External Routable Connectivity~~<u>ERC</u> and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated</u> • <u>EACMS; or</u> • <u>PCA</u>	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, <u>except during CIP Exceptional Circumstances</u>.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-76 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.9	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, <u>except during CIP Exceptional Circumstances</u>.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1—Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.10	High Impact BES Cyber Systems and their associated: - PCA Medium Impact BES Cyber Systems at Control Centers and their associated: - PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: - encryption of data that transits such cabling and components; or - monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or - an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

- R2.** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-~~76~~ Table R2 – Visitor Control Program. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*
- M2.** Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in CIP-006-~~76~~ Table R2 – Visitor Control Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~76~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, ~~except during CIP Exceptional Circumstances.~~	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-76 Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-~~76~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>SCI with ERC hosting Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

- R3.** Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-~~76~~ *Table R3 – Maintenance and Testing Program*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].
- M3.** Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in CIP-006-~~76~~ *Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~76~~ Table R3 – Physical Access Control System Maintenance and Testing Program

Part	Applicable Systems	Requirement	Measures
3.1	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~<u>BCS</u>, ~~or~~ • <u>Medium Impact BES Cyber Systems</u><u>BCS</u> with <u>External Routable Connectivity</u><u>ERC</u> • <u>SCI hosting High Impact BCS or their associated EACMS or PCA; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact ~~BES Cyber Systems~~<u>BCS</u>, ~~or~~ • <u>Medium Impact BES Cyber Systems</u><u>BCS</u> with <u>External Routable Connectivity</u><u>ERC</u> • <u>SCI hosting High Impact BCS or their associated EACMS or PCA; or</u> • <u>SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA</u> <u>SCI hosting PACS associated with High Impact BCS</u> <u>SCI hosting PACS associated with Medium Impact BCS with ERC</u>	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Requirement R1 Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Violation Severity Levels (CIP-006-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R1 Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (Requirement R1 Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (Requirement R1 Part 1.6)

R #	Violation Severity Levels (CIP-006-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption,~~

R #	Violation Severity Levels (CIP-006- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)~~
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Requirement R2 Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact.

R #	Violation Severity Levels (CIP-006-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (Requirement R3 Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (Requirement R3 Part

R #	Violation Severity Levels (CIP-006- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents~~None.~~ See [“Project 2016-02 Virtualization Implementation Plan”](#)**Version History**

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with

Version	Date	Action	Change Tracking
			other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes and CEC language added</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-~~76~~
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (~~BCS~~) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - ~~4.1.4 — Generator Owner~~
 - ~~4.1.54.1.4 — Interchange Coordinator or Interchange Authority~~
 - ~~4.1.64.1.5 — Reliability Coordinator~~

4.1.74.1.6 Transmission Operator**4.1.84.1.7 Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~67~~:

4.2.3.1 Cyber Assets-systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets-systems associated with ~~communication networks and data~~ communication links ~~between discrete~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI). Electronic Security Perimeters.

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.24.2.3.4~~ The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.34.2.3.5~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.6~~ Responsible Entities that identify that they have no ~~BES Cyber Systems~~ BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates:

See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-007-76.~~

~~6. Background:~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training~~

~~program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~High Impact BES Cyber Systems~~ — ~~Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~Medium Impact BES Cyber Systems~~ — ~~Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers**—Only applies to medium impact BES Cyber Systems located at a Control Center.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity**—Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)**—Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)**—Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Protected Cyber Assets (PCA)**—Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~6-7~~ Table R1 – System Hardening~~Ports and Services~~. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*
- M1.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in CIP-007-~~6-7~~ Table R1 – System Hardening~~Ports and Services~~ and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R1— ~~Ports and Services~~ System Hardening			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~<u>BCS</u> with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, Enable only logical-network accessible ports-services~~ that have been determined to be needed by the Responsible Entity, ~~(or logical network accessible ports if unable to determine service,~~ including port ranges ~~or-services~~ where needed to handle dynamic ports), <u>per system capability</u>. -If a ~~device-system~~ has no provision for disabling or restricting <u>network accessible services (or logical ports)</u> ~~on the device~~ then those ~~ports services (or logical ports)~~, that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports, ~~on all applicable Cyber Assets and Electronic Access Points,~~ individually or by group. • Listings of the listening ports, ~~on the Cyber Assets,~~ individually or by group, from either ~~the device~~ configuration files, command output (such as netstat), or network scans of open ports; or • Configuration ~~files~~ of host-based firewalls, ~~- policy,~~ or other ~~device level~~ mechanisms that only allow needed ports and deny all others.

1.2	High Impact ~~BES Cyber Systems~~BCS and their associated ~~PCA~~; and ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated ~~PCA~~; and ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ <u>SCI at Control Centers hosting High or Medium Impact BCS or their associated PCA</u> <u>Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA</u> <u>Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BCS at Control Centers</u>	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
	<u>SCI hosting High or Medium Impact BCS or their associated:</u>	<u>Enable only services that have been determined to be needed by the</u>	<u>Examples of evidence may include, but are not limited to:</u>

CIP-007-76 Table R1— ~~Ports and Services~~ System Hardening			
Part	Applicable Systems	Requirements	Measures
<u>1.3</u>	• <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	<u>Responsible Entity, per system capability.</u>	• <u>Documentation of implemented hardening guidelines</u> • <u>Configuration management reporting</u> <u>that demonstrates the need for all enabled services.</u>

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table R2 – Security Patch Management. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table R2 – Security Patch Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	A patch management process for tracking, evaluating, and installing cyber security patches. ~~for applicable Cyber Assets.~~ The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches <u>for systems for applicable Cyber Assets</u> that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, ~~whether on an individual BES Cyber System or Cyber Asset basis.~~

CIP-007-76 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA;~~and~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA;~~and~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-76 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; ~~or~~ • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-76 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.4	High Impact ~~BES-Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES -Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

- R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table R3 – Malicious Code ~~Protection~~Prevention. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].
- M3.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table R3 – Malicious Code ~~Protection~~Prevention and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R3 – Malicious Code ~~Protection~~ Prevention			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, <u>white-listing</u> , <u>privileged introspection</u> , etc.).

CIP-007-76 Table R3 – Malicious Code ~~Protection~~ Prevention			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-76 Table R3 – Malicious Code ~~Protection~~ Prevention			
Part	Applicable Systems	Requirements	Measures
3.3	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

- R4.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table R4 – Security Event Monitoring. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*
- M4.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table R4 – Security Event Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	Log <u>security</u> events, <u>per system capability, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)</u> for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, ~~at~~ a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BES Cyber System~~BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI with ERC hosting High Impact BCS or Medium Impact BCS with ERC or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules with ERC of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS</u> • <u>EACMS; or</u> • <u>PCA</u>	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, ~~as~~^{at} a minimum, each of the following types of events, ~~(per system or Cyber Asset or BES Cyber System capability)~~: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

4.3	High Impact ~~BES-Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES-Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	~~Where technically feasible,~~Retain applicable <u>security</u> event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, <u>per system or asset capability</u>, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.

CIP-007-76 Table R4 – Security Event Monitoring

Part	Applicable Systems	Requirements	Measures
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

- R5.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table R5 – System Access Controls. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.
- M5.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-007-~~76~~ Table 5 – System Access Controls and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-67 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
5.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) and their associated:	Have a method(s) to enforce authentication of interactive user access, <u>per system capability</u>~~where technically feasible~~.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-67 Table R5 – System Access Controls			
Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA <u>SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS, or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>		
5.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated:	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use ~~for the BES Cyber System.~~

CIP-007-67 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES-Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>		

CIP-007-~~76~~ Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI with ERC hosting High Impact BCS, Medium Impact BCS, or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS, or their associated</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-76 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	Change known default passwords, per ~~system or Cyber Asset~~ capability.	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique ~~to the device.~~

CIP-007-76 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the <u>system</u>~~Cyber Asset~~; and 5.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the <u>system</u>~~Cyber Asset~~.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-76 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI with ERC hosting High Impact BCS, Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS or their associated:</u> • <u>PACS;</u>	~~Where technically feasible, f~~or password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, <u>per system capability</u>.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

	• <u>EACMS; or</u> • <u>PCA</u>		

CIP-007-76 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS or their associated:</u>	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts; <u>or generate alerts after a threshold of unsuccessful authentication attempts, <u>per system capability.</u></u>	Examples of evidence may include, but are not limited to: • Documentation of the account lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

	• <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>		

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.3. Compliance Monitoring and Assessment Processes:

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot-Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

1.4. Additional Compliance Information:

~~None~~

~~Table of Compliance Elements~~**Violation Severity Levels**

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity has implemented and documented processes for ~~Ports and Services~~ <u>System Hardening</u> but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (<u>Requirement R1 Part 1.2</u>)	The Responsible Entity has implemented and documented processes for determining necessary <u>System Hardening</u> ~~Ports and Services~~ <u>but, where technically feasible, but</u> had one or more unneeded ~~logical~~ network accessible ~~services ports~~ enabled. (<u>Requirement R1 Part 1.1</u>) <u>OR</u> <u>The Responsible Entity has implemented and documented processes for determining necessary System Hardening, but had one or more unneeded services enabled. (Requirement R1 Part 1.3)</u>	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007- ~~76~~ Table R1. (<u>Requirement R1</u>)
R2	The Responsible Entity has documented and implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for patch	The Responsible Entity has documented or implemented one or more	The Responsible Entity did not implement or document one or more

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar	management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable ~~Cyber Assets~~systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not	process(es) for patch management but did not include any processes for installing cyber security patches for applicable ~~Cyber Assets~~systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating	process(es) that included the applicable items in CIP-007-76 Table R2. (Requirement R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable ~~Cyber Assets~~systems. (Requirement R2 Part 2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	days of the evaluation completion. (Requirement R2 Part 2.3)	apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (Requirement R2 Part 2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (Requirement R2 Part 2.4)
R3	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		used, the Responsible Entity did not address testing the signatures or patterns. (<u>Requirement R3 Part 3.3</u>)	threat of detected malicious code. (<u>Requirement R3 Part 3.2</u>) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (<u>Requirement R3 Part 3.3</u>).	included the applicable items in CIP-007- ~~76~~ Table R3. (<u>Requirement R3</u>). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (<u>Requirement R3 Part 3.1</u>)
R4	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007- ~~76~~ Table R4. (<u>Requirement R4</u>)

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (Requirement R4 Part 4.4)	calendar days of the prior review. (Requirement R4 Part 4.4)	but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (Requirement R4 Part 4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (~~where technically feasible and~~ except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (Requirement R4 Part 4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an	OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (Requirement R4 Part 4.4)	
R5	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-76 Table R5. (Requirement R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access.

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			identification of the individuals with authorized access to shared accounts. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of	(Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords.

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Requirement R5 Part 5.6)	(Requirement R5 Part 5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for

R #	Violation Severity Levels (CIP-007- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, ~~where technically feasible~~, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- ~~None.~~ [See Project 2016-02 Virtualization Implementation Plan.](#)
- [See Technical Rationale for CIP-007-7](#)

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Virtualization modifications</u>	

Guidelines and Technical Basis

Section 4—Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible (“listening”) ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset’s function, and disable or restrict access to all other ports.

1.1.— This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example—purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed ‘needed.’

~~1.2. — Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for ‘console commands’ primarily means serial ports on Cyber Assets that provide an administrative interface.~~

~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

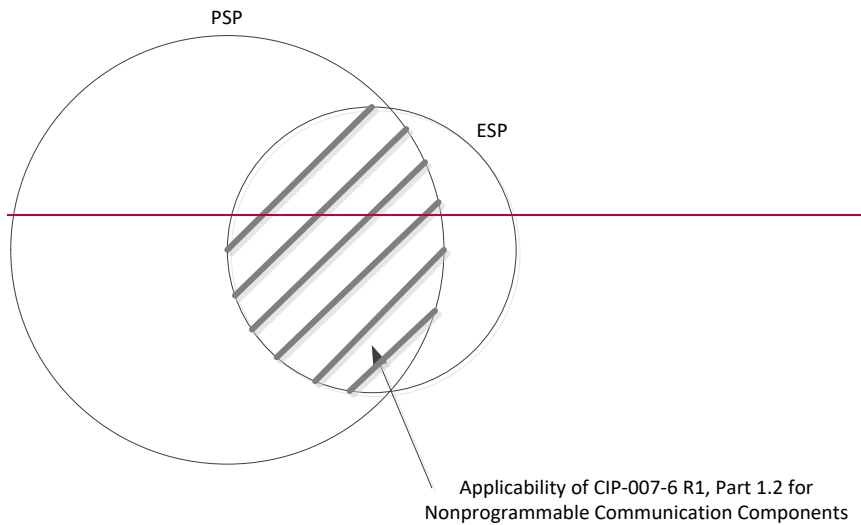
- ~~• Disabling all unneeded physical ports within the Cyber Asset’s configuration~~
- ~~• Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~
- ~~• Physical port obstruction through removable locks~~

~~The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.~~

~~This is a ‘defense in depth’ type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense in depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to “think before you plug anything into one of these systems” which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.~~

~~The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include “Nonprogrammable communication components located inside both a PSP and an ESP.” This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~

Location of Nonprogrammable Communication Components



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

~~can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.~~

~~**2.2.**—Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.3.**—The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

~~those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.~~

~~**2.4.**—The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.~~

Requirement R3:

~~**3.1.**—Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.~~

~~**3.2.**—When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white listing situations, the white listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or~~

~~method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.~~

~~Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP 010-2. The protections required here in CIP 007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.~~

~~**3.3.**—In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System’s ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a ‘false positive’ could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.~~

Requirement R4:

~~Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.~~

~~**4.1.**—In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer-generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.~~

~~Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.~~

~~User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.~~

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~4.2. — Real time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

- ~~• Detected known or potential malware or malicious activity~~
- ~~• Failure of security event logging mechanisms~~
- ~~• Login failures for critical accounts~~
- ~~• Interactive login of system accounts~~
- ~~• Enabling of accounts~~
- ~~• Newly provisioned accounts~~
- ~~• System administration or change tasks by an unauthorized user~~
- ~~• Authentication attempts on certain accounts during non-business hours~~
- ~~• Unauthorized configuration changes~~
- ~~• Insertion of Removable Media in violation of a policy~~

~~4.3 — Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~4.4. — Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

Requirement R5:

Account types referenced in this guidance typically include:

- ~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~
- ~~Individual user account: An account used by a single user.~~
- ~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~
- ~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~
- ~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~
- ~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~
- ~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~
- ~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

5.1 ~~Reference the Requirement's rationale.~~

5.2 ~~Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

5.3 ~~Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

5.4. ~~Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~5.5. — Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, \$, @, &), in various combinations.~~

~~5.6 — Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~5.7 — Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

Rationale:

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

Rationale for Requirement R1:

~~The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE 4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense in depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

Rationale for Requirement R2:

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

Rationale for Requirement R3:

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

Rationale for Requirement R4:

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system-generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard being posted for a 5-day final ballot period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning
2. **Number:** CIP-008-~~76~~
3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Reliability Coordinator**

4.1.6 Transmission Operator**4.1.7 Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:
All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-~~76~~:

4.2.3.1 Cyber ~~Assets-systems~~ at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets-systems~~ associated with communication ~~networks and data communication~~ links ~~between discrete~~

~~Electronic Security Perimeters~~ logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

~~4.2.3.24.2.3.3~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

~~4.2.3.34.2.3.4~~ The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.44.2.3.5~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.6~~ Responsible Entities that identify that they have no BES Cyber Systems ~~(BCS)~~ categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

~~4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.~~

5. Effective Dates:

See ~~“Project 2016-02 Virtualization Implementation Plan.”~~ for CIP-008-76.

6. Background:

~~Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.~~

~~An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~High Impact BES Cyber Systems~~ — ~~Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

~~Medium Impact BES Cyber Systems~~ — ~~Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications.
[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].
- M1.** Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications.

CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS.</u>	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: - A Reportable Cyber Security Incident; or - An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-76 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: • <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS</u>	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

- R2.** Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-76 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].
- M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-76 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-76 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS</u>	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations-based exercises.

CIP-008-76 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES-Cyber-Systems~~BCS and their associated: - EACMS Medium Impact ~~BES-Cyber-Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> - EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact ~~BES-Cyber-Systems~~BCS and their associated: - EACMS Medium Impact ~~BES-Cyber-Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> - EACMS	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column.

- R3.** Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-~~76~~ Table R3 – *Cyber Security Incident Response Plan Review, Update, and Communication*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M3.** Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in CIP-008-~~76~~ Table R3 – *Cyber Security Incident Response Plan Review, Update, and Communication*.

CIP-008-76 Table R3 – Cyber Security Incident Response Plan
Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, ~~all of~~ the following: - Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; - Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and - Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

CIP-008-76 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: - Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and - Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

- R4.** Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC),¹ or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column, unless prohibited by law, in accordance with each of the applicable requirement parts in CIP-008-~~76~~ Table R4 – Notifications and Reporting for Cyber Security Incidents. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M4.** Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column according to the applicable requirement parts in CIP-008-~~76~~ Table R4 – Notifications and Reporting for Cyber Security Incidents.

CIP-008- ~~76~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>EACMS</u>	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

¹ The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

CIP-008-~~76~~ Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.2	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: • <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS</u>	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

CIP-008-76 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.3	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: • <u>EACMS</u> <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS</u>	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment~~ Enforcement Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audit~~
- ~~Self Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self Reporting~~
- ~~Complaint~~

~~1.4. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning	Lower	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Requirement R1 Part 1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (Requirement R1 Part 1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Requirement R1 Part 1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (Requirement R1 Part 1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (Requirement R1 Part 1.2)	from Part 1.2.1, a system identified in the “Applicable Systems” column for Part 1.2. (Requirement R1 Part 1.2)
R2	Operations Planning Real-time Operations	Lower	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months, not exceeding 16 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 17 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 18 calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.2 occurs. (Requirement R2 Part 2.2)	calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.3. (Requirement R2 Part 2.3)
R3	Operations Assessment	Lower	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security	The Responsible Entity has not updated the Cyber Security Incident response plan based on any	The Responsible Entity has neither documented lessons learned nor documented the	The Responsible Entity has neither documented lessons learned nor documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3)	documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3) OR	absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the Cyber Security	absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	Operations Assessment	Lower	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.3 but failed to report on	Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column. (Requirement R4 Part R4)	Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	Reportable Cyber Security Incident. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Requirement R4 Part 4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1.			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Requirement R4 Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ [See "Project 2016-02 Virtualization Implementation Plan."](#)

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems
2. **Number:** CIP-009-~~76~~
3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. **Generator Operator**

4.1.4. Generator Owner~~**4.1.5. Interchange Coordinator or Interchange Authority**~~~~**4.1.6.4.1.5. Reliability Coordinator**~~~~**4.1.7.4.1.6. Transmission Operator**~~~~**4.1.8.4.1.7. Transmission Owner**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Special Protection System or Remedial Action Scheme~~RAS where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-009-~~76~~:

4.2.3.1. Cyber ~~Assets~~systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~systems associated with communication ~~networks and data communication links between discrete Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or Shared Cyber Infrastructure (SCI).

4.2.3.2.4.2.3.3. ~~Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.~~

4.2.3.3.4.2.3.4. ~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.~~

4.2.3.4.4.2.3.5. ~~For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.~~

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~75.1~~ identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan” ~~for CIP-009-76.~~

6. ~~Background:~~ ~~Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.~~

~~An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~**High Impact BES Cyber Systems** — Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** — Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers** — Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** — Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** — Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-~~76~~ Table R1 – Recovery Plan Specifications. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*
- M1.** Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in CIP-009-~~76~~ Table R1 – Recovery Plan Specifications.

CIP-009- ~~76~~ Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009- ~~76~~ Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-76 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	One or more processes for the backup and storage of information required to recover ~~BES Cyber System~~<u>applicable system</u> functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber System~~<u>applicable system</u> functionality.

CIP-009- ~~76~~ Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

CIP-009- ~~76~~ Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.5	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	One or more processes to preserve data, per <u>Cyber Assets</u> system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

- R2.** Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-~~76~~ Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]
- M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in CIP-009-~~76~~ Table R2 – Recovery Plan Implementation and Testing.

CIP-009-76 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-~~76~~ Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~ <u>BCS</u> and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ <u>BCS</u> at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	Test a representative sample of information used to recover ~~BES Cyber System~~ <u>applicable system</u> functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber System~~ <u>applicable system</u> functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-76 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~ BCS SCI hosting High Impact ~~BES Cyber Systems~~ BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

- R3.** Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-~~76~~ Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M3.** Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in CIP-009-~~76~~ Table R3 – Recovery Plan Review, Update and Communication.

CIP-009- ~~76~~ Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers and their associated:</u> <u>PACS; or</u> <u>EACMS</u>	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: - Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; - Dated and revised recovery plan showing any changes based on the lessons learned; and - Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

CIP-009-76 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~ BCS and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: <u>1. PACS; and</u> <u>2. EACMS</u> ~~1. EACMS; and~~ ~~2. PACS~~ <u>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</u> <u>• PACS; or</u> <u>• EACMS</u>	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.4. Compliance Monitoring and Assessment Processes:~~

- ~~• Compliance Audits~~
- ~~• Self-Certifications~~
- ~~• Spot-Checking~~
- ~~• Compliance Investigations~~
- ~~• Self-Reporting~~
- ~~• Complaints~~

~~1.5. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in <u>Requirement R1</u> Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in <u>Requirement R1</u> Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for ~~BES Cyber Systems~~<u>applicable systems</u>. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~<u>applicable systems</u>, but the plan(s) does not address the conditions for activation in <u>Requirement R1</u> Part 1.1. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~<u>applicable systems</u>, but the plan(s) does not address three or more of the requirements in Parts <u>Requirement R1</u> 1.2 through 1.5.

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Requirement R2 Part 2.3)	months between tests. (Requirement R2 Part 2.3)	The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Requirement R2 Part 2.3)	
R3.	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2)	

R #	Violation Severity Levels (CIP-009- ~~76~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			• Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
<u>7</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

Guidelines and Technical Basis

~~Section 4—Scope of Applicability of the CIP Cyber Security Standards~~

~~Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~The following guidelines are available to assist in addressing the required components of a recovery plan:~~

~~NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at~~

~~<http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf>~~

~~National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at~~

~~http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf~~

~~Installation files and media;~~

~~Current backup tapes and any additional documented configuration settings;~~

~~Documented build or restoration procedures; and~~

~~Cross-site replication storage.~~

~~For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not~~

~~required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:~~

~~Periodic (e.g. daily or weekly) backup process—Review generated logs or job status reports and set up notifications for backup failures.~~

~~Non-periodic backup process—If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.~~

~~Data mirroring—Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.~~

~~Manual configuration information—Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.~~

~~The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.~~

~~For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.~~

Requirement R2:

~~A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.~~

~~A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.~~

~~Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."~~

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

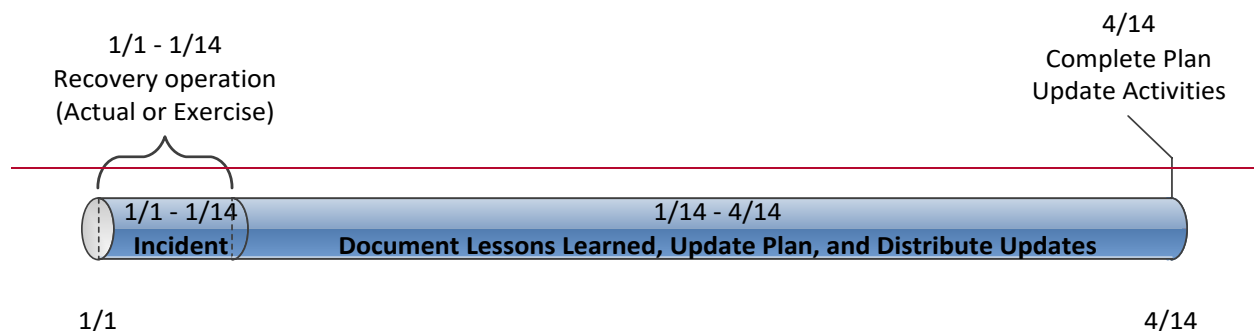


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

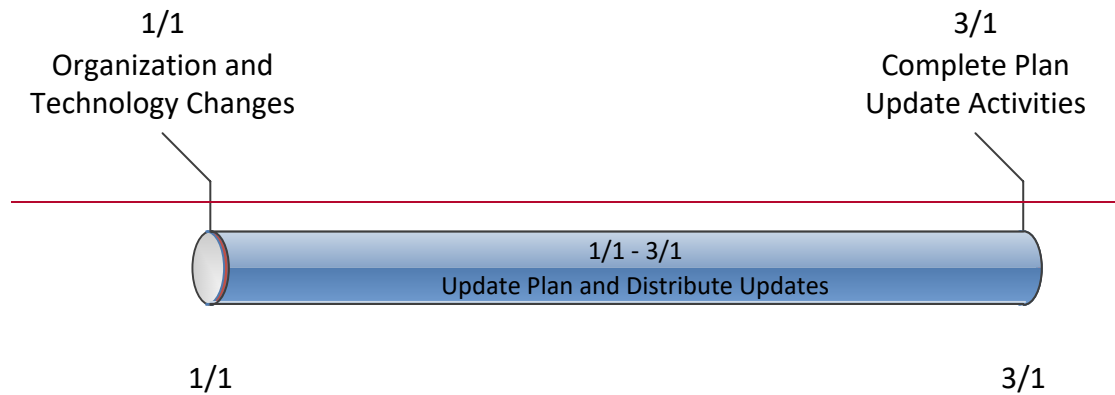


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

Rationale for Requirement R1:

~~Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.~~

Rationale for Requirement R2:

~~The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.~~

~~Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.~~

Rationale for Requirement R3:

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of proposed standard for formal 10-day comment period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — ~~Configuration~~ Change Management and Vulnerability Assessments
2. **Number:** CIP-010-~~54~~
3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. **Generator Operator**

4.1.4. Generator Owner**4.1.5. Reliability Coordinator****4.1.6. Transmission Operator****4.1.7. Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-~~54~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks~~ and data communication links ~~between discrete Electronic~~

~~Security Perimeters~~ logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCL.

~~4.2.3.2.4.2.3.3.~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.4.2.3.4.~~ The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.4.2.3.5.~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.6.~~ Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

~~4.3.~~ **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

~~5.~~ **Effective Date:** See “Project 2016-02 Virtualization Implementation Plan.” for Project 2019-03.

~~**Background:** Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident~~

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described:

High Impact BES Cyber Systems — Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

Medium Impact BES Cyber Systems — Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

~~**Electronic Access Control or Monitoring Systems (EACMS)**—Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)**—Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

~~**Protected Cyber Assets (PCA)**—Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in CIP-010-54 Table R1 – ~~Configuration~~ Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-010-54 Table R1 – ~~Configuration~~ Change Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R1 – ~~Configuration~~ Change Management			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	~~Authorize changes to~~<u>Develop a baseline configuration, individually or by group, which shall include the following items:</u> 1.1.1. Operating system(s) ~~(including version)~~ or firmware ~~where no independent operating system exists~~ <u>or images used to derive operating systems or firmware;</u> 1.1.2. ~~Any e~~Commercially available or open-source application software ~~(including version)~~ <u>intentionally installed including Self-Contained Applications;</u> 1.1.3. ~~Any e~~Custom software installed <u>including Self-Contained Applications;</u> 1.1.4. Any logical network accessible ~~ports~~ <u>services, (or logical ports if unable to determine service);</u>	Examples of evidence may include, but are not limited to: • <u>A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change.</u> ~~A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ ~~A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	<u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	~~and~~ <u>1.1.5. Any Security patches applied;</u> <u>1.1.6. SCI configuration that:</u> • <u>Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI;</u> • <u>-Enforces logical isolation between systems with different impact ratings hosted on SCI;</u> • <u>Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; or</u> • <u>Enables or disables SCI services.</u>	
~~1.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~	~~Authorize and document changes that deviate from the existing baseline configuration.~~	~~Examples of evidence may include, but are not limited to:~~ • ~~A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each~~

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	~~2. PACS; and~~ ~~3. PCA~~		~~change; or~~ ~~• Documentation that the change was performed in accordance with the requirement.~~
~~1.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
~~1.24~~	~~High Impact BES Cyber Systems~~ <u>BCS</u> and their associated: ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems~~ <u>BCS</u> and their associated: ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a each change that deviates from the existing baseline configuration to the items listed in Part 1.1:~~ ~~1.2.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;~~ ~~1.2.2. Following the change, verify that required cyber security controls determined in 1.24.1 are not~~	~~An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.~~

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	<u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	adversely affected; and <u>1.2.3.</u> Document the results of the verification.	
1.35	High Impact BCS <u>SCI hosting High Impact BCS</u>	~~Where technically feasible, for~~ each change ~~that deviates from the existing baseline configuration to the items listed in Part 1.1, per system capability:~~ <u>1.3.1.</u> Prior to implementing any change in the production environment, <u>except during a CIP Exceptional Circumstance</u>, test the changes in a test environment <u>that minimizes differences with the production environment</u> -or test the	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
		changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and <u>1.3.2.</u> Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.64	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS	Prior to a change ~~that deviates from the existing baseline configuration~~ associated with ~~baseline items~~ <u>in Requirement</u> Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: <u>1.46.1.</u> Verify the identity of the software source; and <u>1.46.2.</u> Verify the integrity of the software obtained from the	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	<u>SCI hosting High or Medium Impact BCS and their associated EACMS and PACS.</u> <u>Management Modules of SCI hosting High or Medium Impact BCS and their associated EACMS and PACS.</u> Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.46: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	software source.	

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-4.5 Table R2 – ~~Configuration Change~~ Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-010-4.5 Table R2 – ~~Configuration Change~~ Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R2 – ~~Configuration Change~~ Monitoring			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for ~~unauthorized~~ changes to the ~~baseline configuration (as items~~ described in Requirement R1, Part 1.1}. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

- R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-~~3-5~~ Table R3– *Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*
- M3.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-010-~~3-5~~ Table R3 – *Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4.5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4.5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems <u>SCI hosting High Impact BCS.</u> <u>Management Modules of SCI hosting High Impact BCS.</u>	~~Where technically feasible, a~~ At least once every 36 calendar months, <u>per system capability</u>: 3.2.1 Perform an active vulnerability assessment in a test environment <u>that minimizes differences with the production environment</u>, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, ~~that models the baseline configuration of the BES Cyber System in a production environment~~; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4.5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA <u>SCI hosting High Impact BES Cyber Systems or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PCA</u>	<u>Perform an active vulnerability assessment prior to logically connecting an additional applicable Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure to a production environment, per system capability</u>~~Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset,~~ except for CIP Exceptional Circumstances, <u>or</u> ~~and like replacements~~<u>deployments of the same type of Cyber Asset with</u> using a <u>baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset previously assessed configuration. The production environment does not include devices being actively remediated and logically isolated.</u>	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, <u>Virtual Cyber Asset, or Shared Cyber Infrastructure</u>) and the output of any tools <u>or Management Systems</u> used to perform the assessment.

3.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</u> • <u>PACS;</u> • <u>EACMS; or</u> • <u>PCA</u>	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, <u>a report of Management System actions, or</u> a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

- R4.** Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated SCI and Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*
- M4.** Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a ~~configuration~~-change management process(es) that includes only four <u>or more</u> of the required ~~baseline~~-items listed in 1.1.1 through 1.1.65. (<u>Requirement R1 Part 1.1</u>)	The Responsible Entity has documented and implemented a ~~configuration~~-change management process(es) that includes only three of the required ~~baseline~~-items listed in 1.1.1 through 1.1.65. (<u>Requirement R1 Part 1.1</u>)	The Responsible Entity has documented and implemented a ~~configuration~~-change management process(es) that includes only two of the required ~~baseline~~-items listed in 1.1.1 through 1.1.65. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity has a process as specified in Part 1.64 to verify the identity of the software source (1.64.1) but does not have a process as specified in Part 1.64 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (<u>Requirement R1 Part 1.64.2</u>)	The Responsible Entity has not documented or implemented any ~~configuration~~-change management process(es). (<u>Requirement R1</u>) OR The Responsible Entity has documented and implemented a ~~configuration~~-change management process(es) that includes only one of the required ~~baseline~~-items listed in 1.1.1 through 1.1.65. (<u>Requirement R1 Part 1.1</u>) OR The Responsible Entity does not have a <u>change management</u> process(es) that requires authorization and documentation of changes ~~that deviate from the existing baseline~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~configuration to items listed in 1.1.1-1.1.6. (Requirement R1 Part 1.12)~~ OR ~~The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)~~ OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing ~~baseline~~ configuration. (Requirement R1 Part 1.42.1) OR The Responsible Entity has a process(es) to determine required security controls in

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing ~~baseline~~ configuration but did not verify and document that the required controls were not adversely affected following the change. (<u>Requirement R1 Part 1.42.2</u> & <u>Part 1.42.3</u>) OR The Responsible Entity does not have a process for testing changes ~~in an environment that models the baseline configuration~~ prior to implementing a change ~~that deviates from baseline to the~~ configuration. (<u>Requirement R1 Part 1.53.1</u>) OR The Responsible Entity does not have a process to document the test results and, if using a test

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				environment, document the differences between the test and production environments. (Requirement R1 Part 1.53.2) OR The Responsible Entity does not have a process as specified in Part 1.64 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.64)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to <u>the items described in</u> Requirement R1, Part 1.1.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~the baseline~~ at least once every 35 calendar days. (<u>Requirement R2 Part 2.1</u>)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3 Part 3.1</u>) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for ~~A~~applicable ~~s~~Systems, but has performed an active vulnerability assessment more than 36 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3 Part 3.1</u>) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for ~~a~~Applicable ~~s~~Systems, but has performed an active vulnerability assessment more than 39 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3 Part 3.1</u>) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for ~~a~~Applicable ~~s~~Systems, but has performed an active vulnerability assessment more than 42 months, but	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3</u>) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable ~~BES Cyber S~~systems. (<u>Requirement R3 Part 3.1</u>) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	less than 39 months, since the last active assessment on one of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.2</u>)	less than 42 months, since the last active assessment on one of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.2</u>)	less than 45 months, since the last active assessment on one of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.2</u>)	documented active vulnerability assessment processes for ~~a~~ Applicable ~~s~~ Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.2</u>) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable ~~BES Cyber S~~ systems, but did not perform the active vulnerability assessment ~~in a manner that models an existing baseline configuration~~ of its applicable ~~BES Cyber S~~ systems. (<u>Requirement R3 Part 3.3</u>)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES~~ ~~Cyber-S~~ systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (<u>Requirement R3 Part 3.4</u>)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010- ~~45~~ , Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010- ~~45~~ , Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010- ~~45~~ , Requirement R4,	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010- ~~45~~ , Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Attachment 1, Section 1.1. (Requirement R4 Part R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-45, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	Attachment 1, Section 1.2. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010- ~~45~~ , Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (<u>Requirement</u> R4)	mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010- ~~45~~ , Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (<u>Requirement</u> R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”~~for Project 2019-03.~~
- CIP-010-~~4~~5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	
<u>5</u>	<u>TBD</u>	<u>Virtualization modifications</u>	

CIP-010-54 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

- 1.1. Transient Cyber Asset Management:** Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.
- 1.2. Transient Cyber Asset Authorization:** For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:
 - 1.2.1.** Users, either individually or by group or role;
 - 1.2.2.** Locations, either individually or by group; and
 - 1.2.3.** Uses, which shall be limited to what is necessary to perform business functions.
- 1.3. Software Vulnerability Mitigation:** Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):
 - Security patching, including manual or managed updates;
 - Live operating system and software executable only from read-only media;
 - System hardening; or
 - Other method(s) to mitigate software vulnerabilities.
- 1.4. Introduction of Malicious Code Mitigation:** Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):
 - Antivirus software, including manual or managed updates of signatures or patterns;
 - Application whitelisting; or
 - Other method(s) to mitigate the introduction of malicious code.
- 1.5. Unauthorized Use Mitigation:** Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

- 2.1.** Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):
- Review of installed security patch(es);
 - Review of security patching process used by the party;
 - Review of other vulnerability mitigation performed by the party; or
 - Other method(s) to mitigate software vulnerabilities.
- 2.2.** Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):
- Review of antivirus update level;
 - Review of antivirus update process used by the party;
 - Review of application whitelisting used by the party;
 - Review use of live operating system and software executable only from read-only media;
 - Review of system hardening used by the party; or
 - Other method(s) to mitigate malicious code.
- 2.3.** For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

- 3.1.** Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:
- 3.1.1.** Users, either individually or by group or role; and
- 3.1.2.** Locations, either individually or by group.
- 3.2.** Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

- 3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting to a ~~using a Cyber Asset other than a~~ BES Cyber System or Protected Cyber Assets; and
- 3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-45 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

- Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.
- Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.
- Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
- Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
- Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.
- Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-~~32~~
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. **Generator Operator**
 - 4.1.4. **Generator Owner**

~~4.1.5. Interchange Coordinator or Interchange Authority~~~~4.1.6.4.1.5.~~ Reliability Coordinator~~4.1.7.4.1.6.~~ Transmission Operator~~4.1.8.4.1.7.~~ Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-011-~~32~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic~~

~~Security Perimeters~~ logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCL.

~~4.2.3.2.4.2.3.3.~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.4.2.3.4.~~ The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.4.2.3.5.~~ For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.6.~~ Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-011-32.~~

~~**6. Background:** Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and

~~Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~**High Impact BES Cyber Systems**—Applies to BES Cyber Systems categorized as high impact according to the CIP-002 5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems**—Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 5.1 identification and categorization processes.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)**—Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)**—Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

~~**Protected Cyber Assets (PCA)**—Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-~~32~~ Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M1.** Evidence for the information protection program must include the applicable requirement parts in CIP-011-~~32~~ Table R1 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011- ~~32~~ Table R1 – Information Protection			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems <u>(BCS)</u> and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS.</u>	Method(s) to identify information that meets the definition of ~~BES Cyber System Information~~<u>BCSI</u>.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify ~~BES Cyber System Information~~<u>BCSI</u> from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~<u>BCSI</u> as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize ~~BES Cyber System Information~~<u>BCSI</u>; or • Repository or electronic and physical location designated for housing ~~BES Cyber System Information~~<u>BCSI</u> in the entity's information protection program.

CIP-011-~~32~~ Table R1 – Information Protection

Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~<u>BCS</u> and their associated: 1. EACMS; and 2. PACS <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS; or</u> • <u>PACS</u>	Procedure(s) for protecting and securely handling ~~BES Cyber System Information~~<u>BCSI</u>, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of ~~BES Cyber System Information~~<u>BCSI</u>; or • Records indicating that ~~BES Cyber System Information~~<u>BCSI</u> is handled in a manner consistent with the entity's documented procedure(s).

- R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-~~32~~ Table R2 —~~BES Cyber Asset Reuse and Disposal~~. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-011-~~32~~ Table R2 —~~BES Cyber Asset Reuse and Disposal~~ and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011- ~~32~~ Table R2 — ~~BES Cyber Asset Reuse and Disposal~~			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated:</u> • <u>EACMS;</u> • <u>PACS; or</u> • <u>PCA</u>	<u>Method(s) Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System InformationBCSI from applicable systems prior to upon their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column). outside another applicable systemthe Cyber Asset data storage media.</u>	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of ~~BES Cyber System InformationBCSI~~ such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of ~~BES Cyber System InformationBCSI~~.

CIP-011-~~32~~ Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.2	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence include, but are not limited to:~~ ~~• Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or~~ ~~• Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.~~

C. Compliance

1. Compliance Monitoring Process:

- 1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.
- 1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.3. Compliance Monitoring and Assessment Processes:~~

- ~~• Compliance Audits~~
- ~~• Self-Certifications~~
- ~~• Spot-Checking~~
- ~~• Compliance Violation Investigations~~
- ~~• Self-Reporting~~
- ~~• Complaints~~

~~1.4. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-011- ~~32~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a ~~BES Cyber System Information~~ BCSI protection program (<u>Requirement R1</u>).
R2.	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (<u>Requirement R2 Part 2.1</u>)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (<u>Requirement R2 Part 2.2</u>)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011- ~~32~~ Table R2 – BES Cyber Asset Reuse and Disposal. (<u>Requirement R2</u>)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan. Guideline and Technical Basis (attached).”

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
<u>3</u>	<u>TBD</u>	<u>Virtualization conforming changes</u>	

~~Guidelines and Technical Basis~~

~~Section 4—Scope of Applicability of the CIP Cyber Security Standards~~

~~Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity’s information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity’s BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need to know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

Requirement R2:

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~

~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for~~

~~quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.~~

~~Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.~~

~~In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.~~

~~It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.~~

Rationale

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

Rationale for Requirement R1:

~~The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

Rationale for Requirement R2:

~~The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security - Supply Chain Risk Management
2. **Number:** CIP-013-~~32~~
3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems and their associated cyber systems.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.3. **Generator Operator**
 - 4.1.4. **Generator Owner**
 - 4.1.5. **Reliability Coordinator**
 - 4.1.6. **Transmission Operator**
 - 4.1.7. **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-~~32~~:

4.2.3.1. Cyber ~~Assets-systems~~ at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets-systems~~ associated with communication ~~networks and data communication-links between discrete Electronic Security Perimeters (ESPs)~~ logically isolated from, but not providing logical isolation for, BES Cyber Systems (BCS) or Shared Cyber Infrastructure (SCI).

~~4.2.3.3.~~ Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See "Project 2016-02 Virtualization Implementation Plan."~~for Project 2019-03.~~

B. Requirements and Measures

- R1.** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~BES Cyber Systems~~, ~~and~~ their associated Electronic Access Control or Monitoring Systems (EACMS), ~~and~~ Physical Access Control Systems (PACS), and the SCI hosting high or medium impact BCS or their associated Electronic Access Controlling or Monitoring System (EACMS) or Physical Access Control System (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- 1.1.** One or more process(es) used in planning for the procurement of ~~SCI, BES Cyber Systems~~BCS, and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System (BES) from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
- 1.2.** One or more process(es) used in procuring ~~SCI, BES Cyber Systems~~BCS, and their associated EACMS and PACS, that address the following, as applicable:
- 1.2.1.** Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
- 1.2.2.** Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
- 1.2.3.** Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
- 1.2.4.** Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;
- 1.2.5.** Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the ~~SCI, BES Cyber System~~BCS and their associated EACMS and PACS; and
- 1.2.6.** Coordination of controls for vendor-initiated remote access.
- M1.** Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.
- R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

- M2.** Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.
- R3.** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- M3.** Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

“Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, as specified in Part 1.2, but the plans do not include one of the parts	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, as specified in Part 1.2, but the plans do not include two or more of the parts in <u>Requirement R1</u>	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, as specified in <u>Requirement R1</u> Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~<u>BES Cyber Systems, and their associated EACMS, PACS, and SCI</u>, as specified in <u>Requirement R1</u> Part 1.2.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	in <u>Requirement R1</u> Part 1.2.1 through Part 1.2.6.	Part 1.2.1 through Part 1.2.6.		OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of <del>BES Cyber Systems, and their associated EACMS and PACSBES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring ~~BES Cyber~~</del>	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of <del>BES Cyber Systems, and their associated EACMS and PACSBES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring ~~BES Cyber~~</del>	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACSBES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring~~	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACSBES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Systems and their associated EACMS and PACS~~ BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~Systems and their associated EACMS and PACS~~ BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~BES Cyber Systems and their associated EACMS and PACS~~ BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	~~BES Cyber Systems and their associated EACMS and PACS~~ BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan” ~~for Project 2019-03~~
- ~~CIP-013-2 Technical Rationale~~

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	
<u>3</u>	<u>TBD</u>	<u>Virtualization conforming changes.</u>	

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2017-01 BAL-003 SDT Phase II White Paper

Considerations of Revisions to Address Project
Deliverables

January 6, 2021

RELIABILITY | RESILIENCE | SECURITY



**3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com**

Table of Contents

Preface	iv
Executive Summary.....	1
Introduction	2
Background.....	2
Excerpts from SAR.....	2
<i>Phase I</i>	2
<i>Phase II</i>	2
March 2019 Technical Conference	3
Other Considerations.....	3
Section 1: Overview of Possible New/Modified Requirements	7
Existing Requirements	7
New/Modified BA Requirements	7
Frequency Response Reserves Operational Planning	7
Real-Time Frequency Response Reserves Monitoring	7
Real-Time Frequency Response Reserves Performance.....	7
New GO/GOP Requirements	7
Frequency Responsive Capability	7
Communication to BA.....	7
Frequency Responsive Performance	7
Administrative Changes.....	8
Data Collection.....	8
Form Replacement.....	8
Section 2: Balancing Authority Requirements Options.....	9
Overview.....	9
Operational Planning – Process.....	10
BA-R3	10
BA-M3	10
Justification	10
Operational Planning – Settings	12
BA-R4	12
BA-M4	12
Justification	12
Operational Planning – Exemptions	12

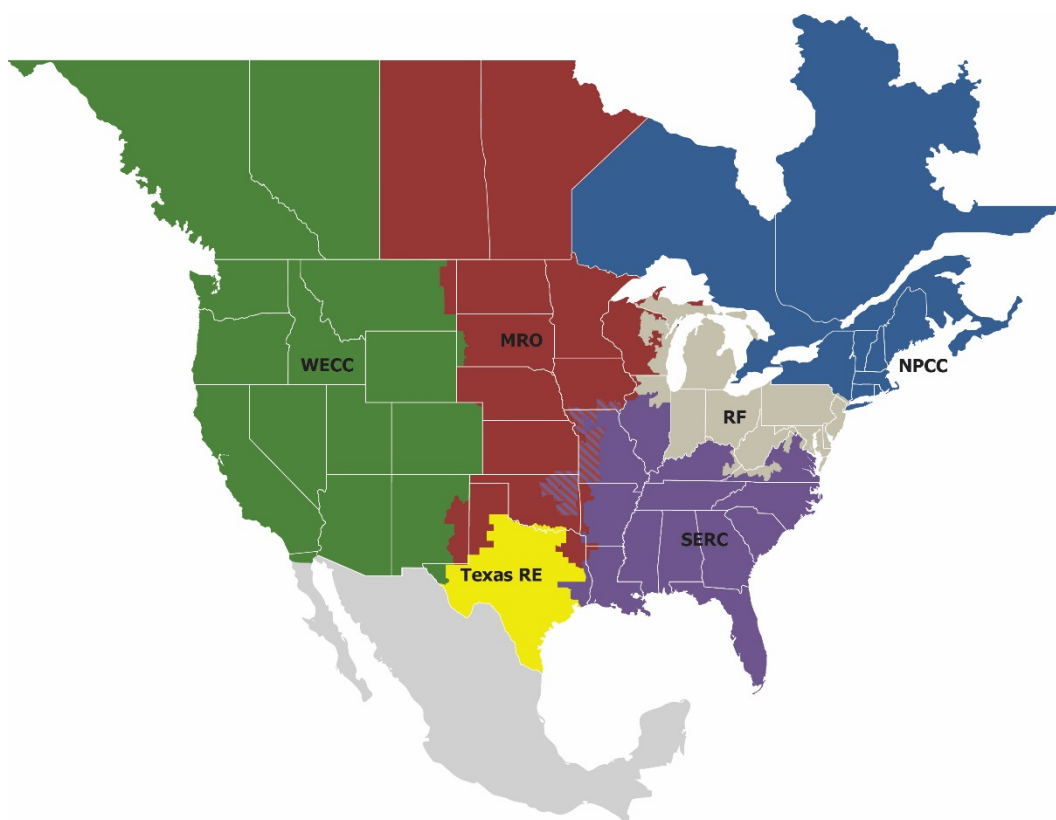
BA-R5	13
BA-M5	13
Justification	13
Section 3: Generator Owner/Generator Operator Requirements Options	14
Overview	14
Resource Frequency Response Performance Requirement	15
Discussion of the Different Options	16
Option 1 – Performance Requirement BA Calculation	16
Option 2 – Performance Requirement GO Calculation	16
Option 3 – Resource Governor In-service Requirement	17
Modes of Operation	18
Resource Frequency Response Communication Requirement	19
Option 4 – Notifications and Governor Settings	19
Consideration of Real-time Information	20
Communication of Governor Settings	20
Requirement to provide the data – Options 4(a) and 4(b)	20
The requirements for providing Frequency Response data to the BA should be considered for all generating resources including but not limited to generators, non-synchronous machines, and storage	20
Settings to be provided, or prescribed	20
Discussion of options: 4(a) and 4(b)	20
Section 4: Summary of Options for Requirements	22
Balancing Authority Requirements	22
R3 – Operational Planning process to schedule adequate Frequency Response reserves	22
R4 - Governor Settings	22
R5 - Governor Setting/Operation Exemption	22
Generator Owner/Operator Requirements	22
Option 1 – Performance Requirement BA Calculation	22
Option 2 – Performance Requirement GO Calculation	22
Option 3 – Resource Governor In-service Requirement	22
Option 4 – Notifications and Governor Settings	23
Conclusion and Recommendations	24
Conclusion	24
Recommendations	24

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Executive Summary

The Project 2017-01 Standard Authorization Request (SAR), under Phase II, directs the standard drafting team (SDT) to consider assigning responsibilities under BAL-003 to different or additional applicable entities, address Real-time operations of the grid, and address measurement concerns, among other things.

The SDT discussed several different options while trying to address the concerns raised in the SAR. These options include potentially adding additional Balancing Authority (BA) requirements to address Real-time primary Frequency Response reserves, modification to existing BA requirements on performance measurements, and adding Generator Owner (GO) and Generator Operator (GOP) requirements for operational and responsive control. These options are detailed in this White Paper.

The SDT is soliciting industry feedback to narrow in on industry's concerns or support of a modification to BAL-003. To facilitate an understanding with industry as to what the SDT has discussed, this paper lays out multiple options. These options are all viable for modifying BAL-003; however, there are certain items that are either mutually inclusive or mutually exclusive, so the final set of requirements proposed for BAL-003 will depend on comments received from industry so the SDT can assess next steps for Project 2017-01, Phase II.

As an initial step, the SDT determined that the BA performance requirement must remain in place for multi-BA Interconnections. While the measurement methodology might change, a requirement on the BA will not be removed. The BAs (or Reserve Sharing Groups, if applicable) have ultimate responsibility for ensuring all reserve requirements are met at the BA level and that there is not another NERC Registered Entity that is in the position to ensure resources are scheduled to provide the needed service.

While some entities have argued that the generators are the ultimate source of the response, the SDT notes that the GOs and GOPs are not able to ensure that any single generator will be committed and dispatched in such a way to allow the generator to respond to an event. This responsibility is that of the BA alone. Therefore, the ultimate responsibility lies with the BA to ensure sufficient Frequency Responsive Reserves are available, just as it is the BA's responsibility to ensure that sufficient Contingency Reserves and Regulating Reserves are available.

The SDT seeks industry feedback on the following proposed requirements:

- New BA requirement – requires Operational Planning process to address Frequency Responsive Reserves
- New BA requirement – specify minimum governor settings or request governor settings from the GO
 - If the BA specifies a governor requirement, then an additional requirement for a process to allow for exceptions would also be recommended by the SDT.
- New GO requirement – Ensure the governor settings meet the BA specification set above
- New GOP requirement – Ensure the unit is operating with the governor and outer loop controls that are responsive or the BA has been notified that it is not responsive.

The SDT considered a generator performance requirement, and that is discussed in detail within this White Paper. If a Frequency Response performance requirement is determined to be proposed for the generators, the SDT believes it would be appropriate for the BAs to calculate the response for each generator within the Balancing Authority Area (BAA), similar to the process found in the BAL-001-TRE-2, Requirement R2.

Reading through this White Paper should help with understanding the reasoning behind the SDT's current position. The SDT looks forward to feedback from industry participants.

Introduction

Background

The issues related to Reliability Standard BAL-003-1.1 were laid out concisely in the SAR. Those issues were grouped into two phases (see SAR excerpts below). The first phase, Phase I, addressed primarily administrative issues. The second phase, Phase II, addresses more complex issues, which contain both administrative and technical elements.

Excerpts from SAR

Phase I

- *Revise the IFRO calculation in BAL-003-1 due to issues identified in the 2016 Frequency Response Annual Analysis (FRAA) Report, such as the Interconnection Frequency Response Obligation (IFRO) values with respect to Point C and varying Value B;*
- *Reevaluate the interconnections' Resource Contingency Protection Criteria;*
- *Reevaluate the frequency nadir point limitations (currently limited to t0 to t+12);*
- *Review and modify as necessary Attachment A of the Reliability Standard to remove administrative tasks and provide additional clarity, e.g., related to Frequency Response Reserve Sharing Groups (FRSG) and the timeline for Frequency Response and Frequency Bias Setting activities; and*
- *Make enhancements to the BAL-003-1.1 FRS Forms that include, but may not be limited to, the ability to collect and submit FRSG performance data.*

In addition to fixing the inconsistencies outlined above, the SDT may separate the administrative and procedural items and propose they be reassigned to an alternative process subject to Electric Reliability Organization (ERO) and North American Electric Reliability (NERC) Operating Committee (OC) approval.

Phase II

- *Both the IFRO calculations and the allocation of IFROs to reliability entities are retrospective (up to 2 years). The review should determine if there are alternate methodologies which consider characteristics affecting Frequency Response (e.g., load response, mix and type of generation, BAA footprint changes) to make allocation as equitable as possible;*
- *Although BAs and FRSGs are responsible for coordination and/or management of Frequency Response from both resources and loads, response from resources is not addressed. The review should determine if additional reliability entities should have responsibility (e.g., GOPs) for provision of generator governor response; and*
- *Review the measurement methodology of Frequency Response (both System and equipment level):*
 - *The FRM should be reviewed to ensure that over-performance by one entity does not negatively impact the evaluation of performance by another.*

All the items in Phase I were addressed in the balloted and approved Reliability Standard BAL-003-2. Although the needed modifications to accommodate FRSG reporting were included in Phase I, additional improvements to the submittal process to further simplify reporting (possibly eliminating mandatory use of the prescribed Excel spreadsheets) were deferred to Phase II.

To clarify the issues needing to be addressed in Phase II, the SDT held a technical conference via WebEx in March of 2019. Here are the questions posed for discussion during the conference and the findings presented by the SDT.

March 2019 Technical Conference

Questions Posed

- What improvements are needed based on Interconnections' performance under the existing BAL-003-1.1?
- Do reliability needs dictate separate measures for Arresting, Stabilizing (current method), and Recovering periods?
- Do the use and application of adjustments (e.g., non-conforming load, dynamic schedules, etc.) need more clarification? Do we need to add other adjustments?
- What are the pitfalls of delta NAI to measure FRM? Are there viable alternatives?
- How can we best simplify the data collection and submittal process?
- Should measurement also include a prospective Frequency Response Reserve (FRR) requirement?
- What areas of historical performance indicate a need for improvement?
- We have seen an improvement in B space with either no change or slight improvement in C space (FRAA Report)?
- Interconnection nadirs (C point) are constant or increasing?
- Particularly, in light of a changing resource mix, what areas of performance in the future need to be addressed?

Findings presented

Findings presented at the conference in response to the questions posed were:

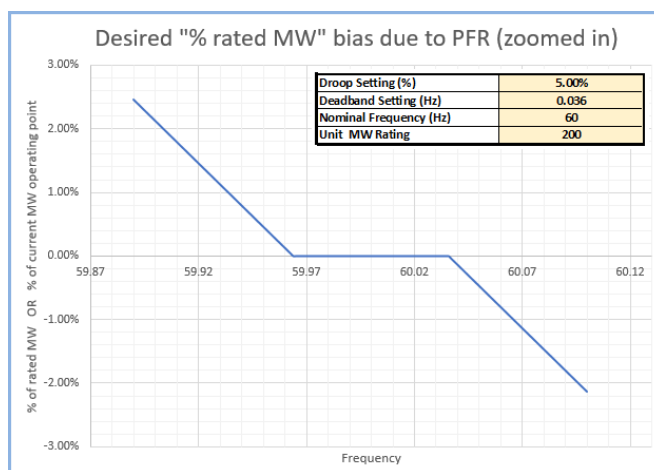
- Although not statistically significant, interconnection performance is stable or slightly improved over the last 4 years (the 2020 FRAA is consistent with the previous 4 years).
- Although the expected future changes in resource mix (driven predominantly by inverter-based resources) will cause changes in the profile over the response period, there is no clear evidence of a reliability need for separate measures (Arresting, Stabilizing, Recovery).
- Clarification of application of adjustments is not needed, but consideration of other adjustments has been made. The administrative burden associated with each (e.g., adjustments for schedule ramping would require coordination of the data submittals of all such schedules between the respective BA partners) precludes the value those identified to date.
- Although the use of NAI (even with existing adjustments) does have limitations and cause inequities for some BAs, no adequate alternative has been identified.
- Data collection and submittal can significantly be simplified. Prototype examples of the submittal forms and corresponding example calculation methods have been developed and are being vetted by the SDT and interested observers.

Other Considerations

This section will provide considerations of other pertinent issues discussed by the SDT during the consideration of the various options for GO/GOP requirements as part of the standard. After describing these other factors, attention will be given to establishing a direction for the SDT with respect to this matter.

Measurement Accuracy

Discussion of the measurement accuracy issues is applicable for interconnection regions where the governor droop and deadband settings are set to 5% droop and +/- 0.036 Hz deadband. Typical non-revenue metering equipment often is known to be 1% accurate. Most sudden imbalance conditions in the Eastern Interconnection do not result in low frequency excursions dropping below 59.9 Hz. The chart below shows the expected % change of facility-rated megawatt (MW) for frequency excursions exceeding the deadband. Notice that the 2% change value occurs at a frequency beyond the majority of the observed frequency excursion limits of the Eastern Interconnection. This results in the situation where the attempted measurement of the frequency responsiveness of many generators in the Eastern Interconnection can be unsuccessful due to the measurement inaccuracies of the equipment in use. Certainly, this can be remedied with projects to use measurement equipment with better accuracy, yet this solution is not without cost and effort. Observed frequency excursions in the Western Interconnection are larger than those in the Eastern Interconnection, so measurement accuracy is a smaller factor in the ability to see the facility response.



Observed frequency excursions

Resource Variability

As mentioned in previous sections, there is **variability in the capability and ability** of existing types of resources to provide primary frequency response due to the modes of operation of those facilities and other important process control constraints. A **generic requirement** which covers existing resource types, therefore, will present GOs with the need for changes in equipment, control modes, efficiencies, and revenue opportunities. In areas where the existing frequency responsiveness is adequate, an application of additional regulations for existing resources may not be warranted. Generic standard requirements for new resource development are more appropriate than detailed, specific requirements. Providing **specific requirements** for certain resource types has the potential to influence, dis-incent, or incent other resource developments in delivering Frequency Response.

Fast Frequency Response

The requirements for fast frequency responsive resources should take into consideration the speed of response characteristics of those resources in comparison to other resources. Certainly, the droop setting controls the

sensitivity of the unit response, and equal sharing of the burden for providing more or less MW for a given frequency excursion will occur given that the excursion lasts long enough for the slowest response timing. If, however, future generating unit resource types with fast Frequency Response become so populous that the MW response needed for arresting and correcting the frequency excursion is available from those fast responding units, the burden would probably not be shared equally with slower responding units even though the droop settings match. At the same time, however, it is understood that those resource types can play an important role during the arresting phase of the frequency excursion.

Frequency Response from New Generation Resources

Provided the trends in the frequency excursion characteristic curve in an interconnection are not markedly showing deterioration coupled with the existing acceptability of the current response, perhaps engaging new generation resources to match the response exhibited by the existing fleet of generators will provide sufficient responsiveness in the future.

The ability to provide sustained Frequency Response from certain types of renewable resources is not guaranteed. Factors include variability in wind speed for wind; operation at maximum power output for wind, solar, steam turbines, and combustion turbines (CTs); intermittent cloud cover for solar; and the current state of charge for battery systems.

The possibility of insufficient Frequency Response stemming from the replacement of traditional synchronous generators (rotating machines) with static-power-conversion-based generation causes focus to be directed towards obligations placed on the new generation to address the issue at the time of the addition of the new resource. The Federal Energy Regulatory Commission (FERC) Order 842 partially addresses this. Interconnection agreements for future resources can specify that all new resources be provisioned with this ability and adequately programmed (controlled) to deliver Frequency Response during normal operation. This ability to have automatic frequency regulation included in the functionality is similar to requiring generating facility equipment to have reactive power production capability, which permits it to deliver automatic voltage regulation (AVR). These provisions, where used and followed, may obviate the need for any additional regulations for GO/GOPs. The adequacy of the existing Frequency Response for the Eastern, Western, and Quebec Interconnections should be considered carefully before new regulation is applied for all generation in each of these interconnections. The frequency excursion characteristics vary from Interconnection to Interconnection.

2017 & 2019 Generator Governor Survey Reports

NERC has performed generator surveys related to frequency response in 2017 and 2019.

These surveys appear to show that generator response to frequency events has increased, although it is still less than expected. It is believed that this increase has been driven due to increased awareness in the industry of the need for frequency response, including efforts by some Balancing Authorities to work with generators to improve response.

TRE Solution

The Texas region has addressed frequency excursion control ability through regional standards specifying governor settings, governor in-service requirements, initial/sustained Frequency Response performance, and credits for load used as a resource (early load shed schemes), and now is developing fast Frequency Response market products.

Market Based Solutions

Many discussions of the growing penetration and density of inverter-based intermittent renewable resources and a forecast of its possible (negative) impact on Frequency Response assumes there is no capability for renewables to provide Frequency Response. This ability may flourish through market requirements and payment for Frequency Response. Market factors would incent the entities to operate these types of resources at less than the maximum available power if properly compensated. Market-driven Frequency Response provision mechanisms can be

developed. These market-based solutions are possibilities instead of provisioning using reliability standard requirements. Both can achieve power injection/withdrawal as needed to regulate the frequency. High-speed power injection and load rejection contracts can arrest frequency declines when dispatched well before the underfrequency load shedding (UFLS) frequency set points in each region. All characteristics of Frequency Response could be incentivized to ensure additional system reliability. BAs may consider acquiring additional Frequency Response through various market means and some resources may elect to participate in market options.

Section 1: Overview of Possible New/Modified Requirements

The rationale for new requirements for both BAs and GOs/GOPs is to have matching requirements for each: one for the operational planning window, one for Real-time status monitoring, and one for performance. The reliability need for each time frame and each functional entity is under much debate.

Existing Requirements

No changes to existing bias setting or measurement reporting requirements.

New/Modified BA Requirements

New BA requirements **may** require a BA to explicitly address planning for Frequency Response reserves in next-day operational planning, develop methods to explicitly monitor Frequency Response reserves in Real-time, and demonstrate Frequency Response reserve maintenance after-the-fact.

Frequency Response Reserves Operational Planning

Explicitly address maintaining Frequency Response reserves in operational plans/procedures.
(See Detail in Chapter 2, R3)

Real-Time Frequency Response Reserves Monitoring

Require BAs to explicitly monitor Frequency Response Reserves in Real-time and to have and meet Real-time targets (static or dynamic). (No formal requirement has been drafted in this paper.)

Real-Time Frequency Response Reserves Performance

Additionally, consideration of an after-the-fact metric on performance (how well did the BA follow its plan?).
(No formal requirement has been drafted in this paper.)

New GO/GOP Requirements

New GO/GOP requirements may require a GO/GOP to explicitly document and communicate Frequency Response capability, develop methods to explicitly monitor and communicate Frequency Response capability in Real-time, and demonstrate Frequency Response performance after-the-fact.

Frequency Responsive Capability

Simple documentation of existence of Frequency Response capability and settings (if capable).

Communication to BA

What information (e.g., just settings or, additionally, actual current capability) should be reported to BA? What mechanism should be used for reporting? And in what periodicity should that information be communicated? All aspects are interrelated (e.g., a one-time settings communication does not need inter-control center communications protocol (ICCP) transfer, but Real-time ramp/headroom capability may).

Is this (could this be) covered by data collection requirements in other standards?

Frequency Responsive Performance

A possible requirement to assess unit performance and meet minimal performance targets.

Administrative Changes

Reporting of data has been reduced to only data needed for multi-BA calculation apportionment and actual required performance metrics. Background data collection, analysis, and calculations are not required to be reported, but prototype calculation methods and tools are developed to provide guidance for users.

Data Collection

A modified spreadsheet form to report needed data for pro rata calculations has been prepared.

Form Replacement

Prototype forms to replace Form 1 and Form 2 have been developed

Section 2: Balancing Authority Requirements Options

Overview

The current Reliability Standard BAL-003-1.1 requires a BA to achieve a median performance on events selected through the frequency event selection process. This process could be thought of as a “past” performance metric since any failure to meet the standard would not be identified until well after the compliance period has passed. This allows the BA to adopt a “wait and see” approach, and puts the interconnection in an assumed state of reliability without any required planning to meet those objectives.

The following requirement was modeled after Reliability Standard VAR-001, Requirement R2, with the intent to move the BA to a forward-looking assessment of available frequency responsive reserves. This is not intended to require the BA to monitor these reserves in Real-time, but simply support a process to evaluate the available Frequency Response in the Operations Planning Horizon, including Real-time operations. While this does not necessarily guarantee performance during an event, it does reduce the risk that a BA might operate in a state with inadequate Frequency Response.

The SDT is proposing a governor (or equivalent control) setting requirement for generating resources connected to the interconnected transmission system. The intent of such a requirement is to:

- Ensure every generating resource is capable of responding to frequency deviations;
- Ensure the BA is aware of the droop and deadband characteristics of the generating resource; and
- Ensure the BA is aware of generating resource operating position and available frequency response.

It has been proposed that a new version, a proposed BAL-003-3, specify the required droop and deadband settings for each generating resource. After careful deliberation, the SDT does not believe it is appropriate to apply a single droop and deadband setting specification to each generating resource. The SDT is proposing that the BA specify the droop and deadband settings and develop an appropriate process for allowing exemptions to the BA’s droop and deadband settings. This process should include exemptions for the governor operating requirement.

The requirement to ensure adequate Frequency Response falls upon the BA. Frequency Response is like other types of Operating Reserve in that a certain amount is necessary to maintain reliability. In the case of Operating Reserve, the BA can choose to carry Operating Reserve on the most effective and efficient resources, while ensuring that there is adequate Operating Reserve in total for the BA. In the same manner, Frequency Response can be procured and dispatched in the most efficient manner across the BA’s entire generating fleet while providing the necessary reliability. Therefore, the SDT elected not to pursue a specific GOP requirement to provide Frequency Response for selected events. Just as there are efficiency and reliability reasons to carry Operating Reserve on specific generating resources, the same logic applies to Frequency Response. Reliability is better served by an analytical approach to provisioning Frequency Response than by requiring each generating resource to provide it at any time for any Frequency Deviation.

Frequency Response is largely determined by the generating resource’s operating point and governor droop and deadband settings. Generating resource types each have unique operating and performance characteristics. For example, when specifying droop, on a hydro generator the control output that changes is gate position. However, a 5% gate change does not equate to a 5% power output change. The same issue applies with Combustion Turbines (CT) and throttle position. The issue becomes more complicated with combined cycle power plants. Generally, the steam turbine does not have a speed governor. Its output varies based on the heat generated (and power) of the CT. In specifying a 5% power droop, if the governor is set to 5%, actual observed power droop is likely to be different. The SDT is proposing that the BA specify droop and deadband settings, which can be based on the BA’s and generating resource’s operating needs and capabilities.

There will be instances where a generating resource is not capable, or it is not desirable to provide Frequency Response. In order to address these cases, the BA shall develop a process that can be applied to determine if a generating resource can be exempted from the requirement to have a governor operating when connected to the interconnected system.

Knowledge of governor status and settings allows the BA to determine the amount of Frequency Response available for any given operating point. With that information, the BA can make the appropriate dispatch decisions to ensure reliability while using the most economic generating resources available. The proposed requirements and the associated justifications describe a coordinated approach to this.

Operational Planning – Process

BA-R3

Each Balancing Authority shall develop and implement an Operating Process, reviewed and maintained at least annually, as part of its Operating Plan to schedule frequency responsive resources sufficient to maintain interconnection frequency equal to or greater than its Frequency Responsive Reserve Obligation.

BA-M3

Each Balancing Authority shall have evidence of scheduling frequency responsive resources based on their assessments of the system. For the operations planning time horizon, Balancing Authorities shall have evidence of assessments used as the basis for how resources were scheduled.

Justification

NERC performed off-peak dynamics analyses of the recommended IFROs for the Eastern, Western, and Texas Interconnections to determine if those levels of primary generator frequency response (PGFR) are adequate to avoid tripping of the first stage of regionally approved UFLS systems in the interconnection. Each of the interconnections prepared light load cases as the starting root case for each of the analyses. In each case, the dynamic governor or load responses of the PGFR of the interconnection closely matched the recommended IFRO value for the prescribed resource loss. All three simulations did not model automatic generation control (AGC), which typically starts to influence PGFR in the 30-45 second timeframe. In all three interconnections analyzed, frequency remained above the highest UFLS set point even with Interconnection PGFR degraded to the IFRO value. The FRAA report presents further analysis of each interconnection for each year.

While the Frequency Response Measure is calculated in MW/.1Hz, the total Frequency Responsive Reserves for each BA should be based on risk associated with anticipated frequency excursions for the applicable interconnection. The responsible entity should have a process to determine the amount of Frequency Responsive Reserves it will plan to have available.

PGFR references and identified risk from the 2012 FRI Report are shown in [Figure 0.1](#) below as an example.

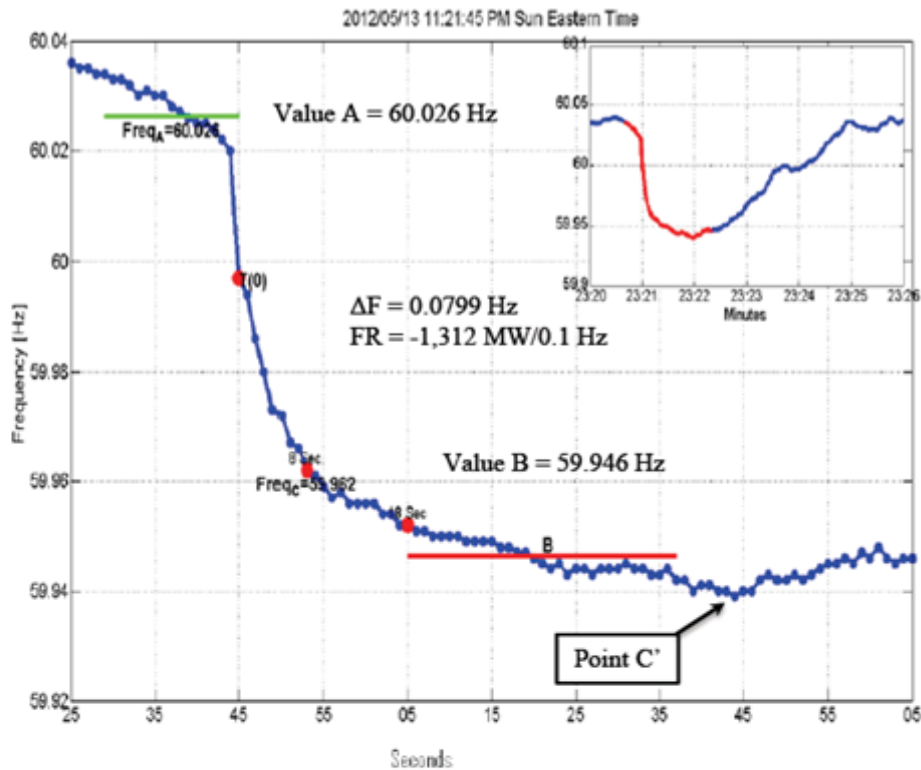


Fig. 24. PGFR Characteristic 11:21 pm Sunday 1,049 MW Resource Loss.

The measurement of Value B (20 to 52 seconds) does not capture the lowest frequency. That frequency point is the true frequency event nadir, hereafter referred to as Point C' ("Point C Prime"), and is normally equal to Point C for events that do not exhibit the so-called "lazy L" effect. It is important that the phenomenon be recorded and trended to determine if it is improving or deteriorating.

NERC Recommendation – Measure and track frequency response sustainability trends by observing frequency between T+45 seconds and T+180 seconds. Calculating a pair of indices comparing that value to both Point C and Value B provides for gauging sustainability. A later alternative comprises the use of arrested PGFR as the PGFR measure.

"NERC should embark immediately on the development of a NERC Frequency Response Resource Guideline to define the performance characteristics expected of those resources for supporting reliability. That guideline should address appropriate parameters for the following:

Figure 0.1: Excerpt from FRI Report October 2012

While these studies assure us that our past performance in each interconnection has been sufficient, they do not necessarily represent the changing resource mix and the potential future performance. This also covers a gap where the BA is required to plan for and carry Contingency Reserves but where those reserves may not be frequency responsive, making them irrelevant to stabilizing the system immediately after a resource loss. In addition to this standard, the Operating Reserve Reliability Guideline should be updated with examples on how to calculate Frequency Response similar to the Electric Reliability Council of Texas (ERCOT) approach with BAL-001-TRE. With the time it takes to modify a standard to address these potential issues in the future, the timing is right to address these known risks now before the interconnections approach a more critical situation.

Operational Planning – Settings

BA-R4

Each Balancing Authority shall specify a minimum droop and deadband setting for the resources located within its boundaries and provide those minimum settings to the Generator Owner.

R4.1

Each Balancing Authority shall provide a copy of the minimum droop and deadband settings to its Reliability Coordinator and adjacent Balancing Authorities within 30 calendar days of a request.

BA-M4

Each Balancing Authority shall have evidence that it specified resource droop, deadband, or equivalent control settings to its resources.

- Each Balancing Authority shall have evidence that the frequency control specifications were provided to its Reliability Coordinator and adjacent Balancing Authorities within 30 calendar days of a request. Evidence may include but is not limited to emails, website postings, and meeting minutes.

Justification

The intent of these proposed requirements is to assist the BA in developing criteria for determining compliance with Requirement R3.

This model is different than the other ancillary services products currently obtained and utilized by BAs to ensure reliability services are available, and it may negatively impact other possible sources of Frequency Response due to lack of compensation. There is also some concern about how generators will be compensated for changes required by its BA, and that the process could be manipulated by a BA by assigning response to certain generators and then limiting dispatch of those generators. But this model simplifies the modeling and operational analysis and allows BAs to require specific settings.

Operational Planning – Exemptions

BA-R5

Each Balancing Authority shall specify the criteria that will exempt generators from:

1. Following the recommended governor droop and deadband settings;
2. Having its governors in service and not blocked; and
3. Having to make associated notifications on governor status changes.

If a Balancing Authority determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

BA-M5

Each Balancing Authority shall have evidence of documenting criteria for generator exemptions and documentation of notifications to exempted resources.

Justification

The previous Requirement R4, sets the expectations for resources, and R5 addresses the known limitations that prevent every resource from providing Frequency Response. Requirements R4 and R5 support Requirement R3, which is ultimately needed to comply with Requirement R1. This exemption process should identify resource types that have known mechanical or safety limits to performing Frequency Response. This process also completes the communication loop between the BA and GOP. Other standards are being discussed for the GOP's requirement to perform.

Section 3: Generator Owner/Generator Operator Requirements Options

Overview

Considerable discussion has occurred in recent years of possible requirements for the GO/GOP in the NERC functional model related to improving the ability to control the frequency of an Interconnection during system disturbances. The Frequency Response provided by connected generation and loads during the first minute(s) following a sudden, unplanned upset between the balance of generation and load plays a vital role in arresting the change in system frequency that results from the imbalance.

This section will address four options for engaging the GO/GOP in system frequency management, which is currently required of the BA through the BAL family of NERC Reliability Standards. Since the BA is tasked with frequency control, BA knowledge of the expected Frequency Response that should occur for disturbances can provide confidence in its ability to meet the frequency control obligations. While presenting various methods for this engagement, the following will be discussed:

- the present and forecasted system need for changes in the GO/GOP Frequency Response performance;
- the level of engagement of GO/GOP for delivering Frequency Response – adequacy issues;
- the changing mix of generating facility resource types, their operating/response characteristics, and their impact on Frequency Response in relation to system inertia and reserves;
- information/communication-based requirements versus measured performance requirements; and
- the ability to use market products for soliciting/ensuring adequate provision of Frequency Response.

Changes in the resource mix of electric power generating facilities tend to change the grid dynamics relative to frequency control capability. Lower system inertia results in increased rate-of-change-of-frequency when sudden imbalances in generation and load occur. Each interconnection currently maintains adequate and substantial margin between automatic UFLS set-points and the lowest frequencies experienced in recent years. Many new resource types can be controlled such that they can provide Frequency Response. Many existing synchronous resource types have been modified in the past decade to provide reliable Frequency Response. The present and forecasted system need for Frequency Response and the response capability of resources are closely related issues.

Options that the SDT has discussed include:

1. Copy all BAL-001-TRE performance requirements, including the requirement for the BA to calculate the response for all generators within their BA footprint. (**Option 1** below.)
2. Create GO/GOP performance requirements with the GO/GOP responsible for the calculation of the performance. (**Option 2** below.)
3. Limit the GO/GOP requirements to just “Operate with the Governor in Service” and “Notify if out of service” only. (**Option 3** below.)
4. Create requirements for the GO/GOP to provide the droop, deadband and other requested data to the BA. (**Option 4** below.)
5. A combination of 3 and 4 above

Each possible method of addressing the GO/GOP in frequency control through the regulatory process that has been discussed by the BAL-003 SDT under Project 2017-03 will be examined and evaluated in this document.

Resource Frequency Response Performance Requirement

The Project 2017-01 SDT has discussed whether it would be appropriate for GO/GOP requirements to replace the current BA requirement due to comments received during the SAR process. During discussions, the SDT determined:

1. The largest BAs in the Eastern and the Western Interconnections are responsible for determining the commitment and dispatch levels of unassociated generation within their footprint during Real-time operations. Therefore, without a BA requirement to ensure the generation fleet is committed and dispatched in a manner to allow response, the GO/GOP would be at risk of meeting a requirement that would replace the current BA requirement while the generation could be committed and/or dispatched such that all available generation meets the performance requirement but the interconnection fails to have sufficient response.
2. Allocating the IFRO to GO/GOPs would either require a Real-time allocation process to address units on and off-line or be likely to aggravate minimum load/generation balancing issues already seen at times as GO/GOPs would need to keep some generation online to provide the required response.

For these reasons, the SDT determined that a GO/GOP requirement could not replace the existing BA requirement. Instead, any GO/GOP requirement would have to be in addition to the existing BA requirement. Therefore, the SDT has focused its discussions in this direction.

This possible set of requirements would be like some or all of those that exist today in the Texas Reliability Entity (TRE) regional standard, BAL-001-TRE-2. Individual resources, whether a single generating unit or an aggregated group of resources such as a wind farm, would be measured against an expected level of response during identified frequency events to determine if the resources are responding.

For ease of understanding and reference, a summary of the pertinent TRE requirements is provided:

- R2 – BA calculates the Frequency Response (both initial and sustained) for each generator;
- R6 - GO must set controls to meet three criteria: droop, deadband and slope;
- R7 – GO shall operate the generator with the governor in-service unless there is a valid reason for it to be out-of-service and the GOP has been notified.
- R8 – GOP will notify the BA within 30 minutes of change in status of the governor.
- R9 – GO will meet 12 month rolling average initial Frequency Response performance of 0.75 based on participation in at least 8 events.
- R10 – GO will meet 12 month rolling average sustained Frequency Response performance of 0.75 based on participation in at least 8 events.

The SDT notes that the TRE standard does not have a BA performance requirement. However, ERCOT, as the registered BA, does have a performance requirement under the NERC BAL-003 standard.

Discussion of the Different Options

Option 1 – Performance Requirement BA Calculation

Under Option 1 above, the SDT discussed the benefits, possible hurdles and perceived negatives associated with the potential requirements structure. These are listed below:

Benefits

- The requirements are relatively clear and understood.
- Data available from TRE shows the process provides an adequate level of reliability.
- Expectation that the amount of Frequency Response seen would remain steady or increase regardless of changes in the generation mix.

Possible Hurdles

- Data transfer rates between generators and BAs in many areas may not be sufficient to allow the BA to make the calculation. (ERCOT uses a 1-second data transfer rate compared to 2-to-6 seconds in other BAs).
- Calculation process may be onerous for smaller BAs.
- Generators may incur expenses to address performance requirements with no clear process for compensation.
- Interconnection size may impede the ability to identify a significant number of events that exceed the deadband.

Negatives

- For BAs with large geographic areas, Frequency Deviations across the system may cause complications for the calculation process.
- Potential for penalizing GO/GOP when more than adequate response across the BA and interconnection is provided (even if the BA and GO/GOP are the same entity).
- Compliance burden may be greater than the potential reliability benefit by placing a compliance obligation on all GO/GOP when over multiple years actual response comes from 50 percent or fewer of units.
- Mandatory performance without clear compensation may negatively impact development of alternative providers of Frequency Response.

Option 2 – Performance Requirement GO Calculation

Under Option 2, the identified list of benefits, possible hurdles and negatives are much the same. The main differences would be related to the data transfer rate and geographic issues and depends on whether the BA, or the GO, would be responsible for calculations. Regardless, the larger number of entities involved in the calculation process would likely increase the administrative burden of the process.

Benefits

- Clear and relatively easy to understand.
- Data available showing experience in TRE to support adequacy of the process.

- Increased Frequency Response.
- May provide reliability value if proven to be needed.

Possible Hurdles

- Calculation process may be onerous for smaller GO/GOPs.
- Generators may incur expenses to address performance requirements with no clear process for compensation.
- Data needed to make the calculation at the GO/GOP level may require significant modifications to data collection at the plant level.
- Interconnection size may impede the ability to identify a significant enough number of events that exceed the deadband.

Negatives

- Large number of entities required to have the data necessary for the calculation, and maintaining trained individuals to perform the calculation may cause the process to be administratively burdensome.
- Potential for penalizing GO/GOP when more than adequate response across the BA and interconnection is provided (even if the BA and GO/GOP are the same entity).
- Compliance burden may be greater than the potential reliability benefit by placing a compliance obligation on all GO/GOPs when, over multiple years, the actual response comes from 50 percent or fewer of units.
- Mandatory performance without clear compensation may negatively impact development of alternative providers of Frequency Response.

BAL-001-TRE-1 became effective on April 1, 2014. Under the standard, a generator must participate in a minimum of 8 frequency events to have a measurable performance obligation. As of August 1, 2020, approximately 20 percent of the generators in the TRE footprint have been scored on 8 or more events. Of the remaining generators, 24.3 percent have received a score in less than 8 events and 55.7 percent have not received a score in any event; therefore, at this time they do not have an official compliance obligation for performance. All generators have an obligation under the standard to have the required settings in place, regardless of event participation.

Option 3 – Resource Governor In-service Requirement

This possible requirement for the GO/GOP for frequency control can be compared with Reliability Standard VAR-002, which is concerned with voltage control. Reliability Standard VAR-002, in paraphrase, obligates the GO or GOP to:

- operate each generator with the automatic voltage regulator in-service and controlling voltage;
- maintain the voltage or reactive schedule provided by the TOP;
- modify voltage when instructed or provide an explanation for not being able to do so;
- notify the TOP of AVR, PSS, or voltage controlling device status changes;
- notify the TOP of reactive capability status changes;
- provide GSU and Aux transformer tap settings, ranges, and transformer impedance data to the TOP and TP;
- modify GSU transformer tap settings, if possible, at the request of the TOP; and

- follow alternate directions by the TOP, or be exempted due to being in startup, shutdown, or testing mode.

Whereas the requirements of Reliability Standard VAR-002 apply to the AVR equipment located at generating facilities for the purpose of voltage control, possible requirements of a proposed BAL-003-3 could apply to the turbine/plant control systems to promote system frequency control and stability. These requirements could take the form of the following:

- operate each governor/speed/frequency/MW set point controller with the primary frequency regulator in-service and controlling frequency;
- maintain the scheduled frequency using a proportional control with percent droop and frequency deadband; settings (see the next section for a discussion of specifying and/or reporting the settings between the GO/GOP and the BA);
- provide an explanation to the BA for not being able to contribute to frequency control;
- notify the BA of frequency controlling device status changes;
- provide the in-service frequency controlling device settings to the BA;
- modify the in-service frequency controlling device settings, if possible, at the request of the BA; and
- follow alternate directions by the BA, or be exempted due to being in startup, shutdown, or testing modes.

FERC Order 842 requires minimum interconnection requirements for new units/facilities, including the installation, maintenance, and operation of a functioning governor. The first bullet above is akin to that part of FERC Order 842. There is significant debate about whether, given the current state of acceptable frequency responsiveness, new resource requirements to provide Frequency Response will provide adequate ability to arrest and correct future frequency disturbances.

In the above-bulleted list of possible GO/GOP requirements, several are informational in nature, where the GO/GOP is providing information to the BA on the ability to control frequency (providing an explanation of not being able to control frequency, notifying due to status changes, etc.). Where the BA wants this information to use for a reliability purpose, the BA may require it through the data specifications developed under Reliability Standard TOP-003. Considering a GO/GOP requirement to provide information that has not previously been required (by Reliability Standard TOP-003) raises the question of whether the information will be used for any purpose.

This requirement is one which can be "coupled" with new BA requirements for having a Frequency Response reserve plan, knowing the Frequency Response reserves available. Although traditional generation does not have on/off switches for governors, differing vastly from AVR control modes, improper settings can defeat an otherwise responsive governor. A turbine control system may not have system frequency (speed) built into the governor during on-line operation. Examples of this are steam valve position and hydro wicket gate position regulators. Solar and wind generating facilities often operate at the maximum power operating point and, therefore, are unable to provide any additional response for underfrequency disturbances. Additionally, the variability of the power source for these types of facilities prevents certainty of the 100% availability for Frequency Response. Certain steam turbine driven generators operate with the turbine steam valves in a wide-open position which will prevent additional generation from being available for underfrequency events. Some CT controllers run fuel control at a maximum exhaust temperature mode which may prevent additional generation from being available for underfrequency events.

Modes of Operation

The following is a discussion of the ability to implement possible requirements ("Options") outlined above and provides considerations relevant to each. Operating each governor or equivalent controller with the primary

frequency regulator in-service and controlling frequency, in most cases, should not be a difficult proposition due to the following characteristics of most control systems:

- A frequency-dependent bias component exists in the control equipment functionality; and
- In-service/out-of-service control switches or variable parameter settings permit the tuning and detuning of the responsiveness of the frequency-dependent bias component.

There could, however, be other important process elements or operating modes which may serve to eliminate, either partially or wholly, the ability of this frequency-dependent bias component from providing the desired Frequency Response during frequency disturbances. These include, but are not limited to:

- The importance of and focus given to reactor controls at nuclear generating stations.
 - Some controls on these units have shown the ability to provide Frequency Response, while others intentionally have detuned the controls by various methods to prevent their operation, thereby increasing the stability of the reactor control.
- Current, widely-used modes of operation for wind, solar, CTs, and steam turbines may permit or may restrict responsiveness. These modes include:
 - operation at the maximum power point (solar, wind, batteries, steam turbines, CTs, etc.);
 - operating at the minimum power point in the control continuum;
 - CT running at the maximum allowable exhaust temperature limit; and
 - coal-fired unit on the verge of coal requirement switching point to change load levels.

Prescribed changes to the modes of operation would be necessary in these instances to permit the existing equipment to provide Frequency Response. Maintaining the scheduled frequency using frequency-dependent bias components with specified limits to the sensitivity settings has been shown to be possible where generating units are not constrained by other operational limitations. A discussion of the sensitivity settings (droop, deadband) is part of the next section of this document.

Resource Frequency Response Communication Requirement

Option 4 – Notifications and Governor Settings

Notifications by the GO/GOP to the BA could be provided to indicate the ability of a unit, or change in the ability of a unit, to provide Frequency Response. For each unit, operational experience and certain test results can provide this intelligence which can be conveyed to the BA for use in frequency response reserve planning. Many generating units will have known operating conditions where Frequency Response can be expected. Additionally, operating conditions resulting in no Frequency Response are often known. Real-time determination and communication of these instances would prove to be more challenging in some cases, as there may be difficulty or uncertainty in incorporating all aspects of unit operating conditions into the logic used to indicate the expected responsiveness. Where on/off switches are used in control systems for the frequency responsive component of the control, changes to the set points of the control can easily be communicated to the BA.

Providing the in-service frequency controlling device settings to the BA is expected to be a one-time event as these settings are not often modified. Modifying these settings is possible and are recommended to be changed while the controller is not in service. Requiring a unit to be offline for these changes impacts the speed in which changes can be implemented. Consideration should be given to the variation in droop and deadband settings of governor primary frequency control settings for all generating units in each interconnection. A coordinated approach for contributions from each facility during Frequency Disturbances is desired. A secondary effect of any changes to the droop and

deadband settings could cause the model verification performed as part of Reliability Standard MOD-027 to become invalid, and this would trigger a requirement to re-verify that model.

Exceptions to any prescribed Frequency Response requirement for the GO/GOP need to be considered and permitted for certain situations. These include unique unit attributes allowed for alternate directions by the BA, being in startup, shutdown, or testing modes, or other individual peculiarities or anomalies that exist with a generating facility. These types of exceptions are analogous to voltage schedule adherence exceptions which are allowed under Reliability Standard VAR-002. Communication and discussion of these exceptions should be expected between the GO/GOP and the BA.

Consideration of Real-time Information

Generating units providing Real-time information to BAs on the available Frequency Response capability would provide valuable transparency to the expected Frequency Response. The SDT has discussed a BA requirement (see Section 1: New/Modified BA Requirement) to calculate and have available a set amount of Frequency Response reserves in Real-time. A requirement for the generating units to provide information to the BA on the capability would be a direct complement to this requirement. No BA requirement for Real-time Frequency Response reserves determination was drafted.

Communication of Governor Settings

Areas the SDT has been discussing around the topic of Real-time status, availability, and expected droop and deadband settings are:

- Requirement to provide the data;
- Settings to be provided, or prescribed; and
- What parameters should to be communicated.

Requirement to provide the data – Options 4(a) and 4(b)

The requirements for providing Frequency Response data to the BA should be considered for all generating resources including but not limited to generators, non-synchronous machines, and storage.

Options discussed by the SDT for a requirement to provide Real-time Frequency Response data were:

Option 4(a): Add a new BA requirement in Reliability Standard BAL-003.

Option 4(b): Provide recommendation for information to be provided under Reliability Standard TOP- 003.

Settings to be provided, or prescribed

Options discussed by the SDT on the droop and deadband settings information to be provided were:

1. The droop and deadband settings can be specified to the generator by the BA.
2. The GO would communicate the current droop and deadband settings of the unit to the BA.

Discussion of options: 4(a) and 4(b)

Under Option 4(a), a new requirement would be added to Reliability Standard BAL-003 for the BA to provide the specified Frequency Response communications to the GO. The BA would be able to set the required droop and deadband for all resources (see Section 2, BA R4). BAs would need to determine if they required the “default” deadband (no greater than 36 MHz), and droop (no greater than 5%), or if there were different settings that would be appropriate. It will also need to be determined if a resource type would drive the Frequency Response setting and

an exception process would need to be considered for resources unable to provide Frequency Response (See Chapter 2, BA R5).

Benefits

- Ensures the BA knows what to expect from all generators in its footprint;
- Allows BAs to set requirements aligned with ensuring adequate Frequency Response capability is available on the system; and
- Would minimize the information that would need to be provided in Real-time from the GO to the BA.

Possible Hurdles

- Requires BAs to put processes in-place to define the required droop and deadband settings;
- Could require measurable staff support to respond to generator inquiries and potential discrepancies between generator capabilities and requirements.

Negatives

- Potential concerns over large discrepancies between BAs on requirements for droop and deadband settings; and
- Potential concerns over fairness between all generators in a given BA, and potentially different settings or exemptions between resource types.

Under Option 4(b), the GO would communicate to the BA the current droop and deadband settings of the unit. There would not be a set droop or deadband expectation for the resources. Rather, this would ensure the transparency of the resource capability and operations. The Frequency Response communications from the GO/GOP to the BA would be managed under the existing (or modified) TOP-003 Reliability Standard. A benefit to this method is that existing processes and data exchange can be used to provide the additional data. A hurdle to this method may be that a new SAR for modification to the existing TOP-003 Reliability Standard may be needed to allow for this data to fit within the requirements. Adding data requirements without a clear understanding of how this data will be used by the BA does not fulfill the contemplated requirements for the BA documented in Sections 1 and 2.

Benefits

- Would allow the BA to have situational awareness of available Frequency Response reserves; and
- Minimal cost to implement communication of the droop and deadband settings.

Possible Hurdles

- This information is already being communicated to the Transmission Planner as part of the Reliability Standard MOD-027 data; and
- Determination needs to be made as to whether this data would be usable by the BA, or if this data would not be valid for Real-time awareness and reserve calculations.

Negatives

- Potential to have significant data exchange requirements between the generator and BA; and
- While increasing visibility, this requirement would not necessarily increase Frequency Response.

Section 4: Summary of Options for Requirements

Balancing Authority Requirements

R3 – Operational Planning process to schedule adequate Frequency Response reserves

- A. **BA-R3:** Each Balancing Authority shall develop and implement an Operating Process, reviewed and maintained at least annually, as part of its Operating Plan to schedule frequency responsive resources sufficient to maintain interconnection frequency equal to or greater than its frequency responsive reserve obligation.

R4 - Governor Settings

- A. **BA-R4:** BA specifies minimum Governor Settings in its appropriate data specification (droop, deadband, and operating mode) for Generators within BA Footprint.
- B. **BA-R4.1** Each Balancing Authority shall provide a copy of the minimum droop and deadband settings to its Reliability Coordinator and adjacent Balancing Authorities within 30 calendar days of a request.

To be able to plan and schedule sufficient Frequency Response reserves, BAs will need actual governor settings from each generator in their footprint. Where should any potential request for data (droop, deadband, and operating mode) from the GO/GOP to the BA be addressed?

R5 - Governor Setting/Operation Exemption

- A. **BA R5:** The Balancing Authority specifies exemption process for governor settings (droop, deadband, and operating mode) in BA R4.

Generator Owner/Operator Requirements

Option 1 – Performance Requirement BA Calculation

Requirements similar to BAL-001-TRE where the local BA performs the generator performance calculations.

Option 2 – Performance Requirement GO Calculation

Requirements similar to BAL-001-TRE where the GO/GOP performs the generator performance calculations.

Option 3 – Resource Governor In-service Requirement

Requirements similar to VAR-002 for voltage control equipment applied to the turbine/plant speed / MW/frequency control systems. These requirements may take the form of the following:

- operate each governor/speed/frequency/MW set point controller with the primary frequency regulator in-service and controlling frequency;
- maintain the scheduled frequency using a proportional control with percent droop and frequency deadband; settings (see the next section for a discussion of specifying and/or reporting the settings between the GO/GOP and the BA);

- provide an explanation to the BA for not being able to contribute to frequency control;
- notify the BA of frequency controlling device status changes;
- provide the in-service frequency controlling device settings to the BA;
- modify the in-service frequency controlling device settings, if possible, at the request of the BA; and
- follow alternate directions by the BA, or be exempted due to being in startup, shutdown, or testing modes.

Option 4 – Notifications and Governor Settings

This possible requirement would require

- notifications by the GO/GOP to the BA could be provided to indicate the ability of a unit, or change in the ability of a unit, to provide Frequency Response
- Providing the in-service frequency controlling device settings to the BA. Two methods of this communication are being considered:
 - a. The droop and deadband settings can be specified to the generator by the BA.
 - b. The GO would communicate the current droop and deadband settings of the unit to the BA.

Conclusion and Recommendations

Conclusion

Various methodologies are available for the establishment of systems to arrest, stabilize, and restore to normal any sudden imbalances in generation and load which manifest themselves in Frequency Disturbances. This White Paper has investigated several methods as possible approaches that are detailed in Chapters 2 and 3. Additionally, other relevant considerations including varying existing resource capabilities, new technology capabilities, existing Frequency Response adequacy measures, projected Frequency Response adequacy estimations, and market solutions have been presented.

Recommendations

The SDT recommends a four-layered approach to provide for the adequacy of Frequency Response resources:

1. Require BAs to gather information on a GO's ability to provide Frequency Response, where needed, to permit improved Frequency Response reserves planning.
2. Limit the GO/GOP national standard requirement for frequency control to one that is similar to the existing GO/GOP requirement for the provision of voltage control for resources with the ability to perform the function.
3. Allow the provisions contained with the FERC Order 842, coupled with Interconnection Agreements for future connected resources, to procure and establish additional frequency responsiveness. New resources with this capability included in the functionality allow for marketplace solutions.
4. Permit the establishment of market incentives for areas/regions where additional reserve is desired.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
~~45-day formal comment period with ballot~~	~~August 6 – September 21, 2020~~
~~45-day formal comment period with ballot~~	~~March 25 – May 10, 2021~~

Anticipated Actions	Date
~~45-day formal comment period with additional ballot~~	~~August 2020~~
10-day final ballot	~~September-May 2021~~ ₀
Board adoption	November 2021 ₀

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-~~X7~~
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, ~~and~~ security awareness, and access management in support of protecting BES Cyber Systems.

4. Applicability:

- 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

- 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

- 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

- 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

- 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

- 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

- 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~X7~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1a identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-~~X7~~.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” ~~or “Applicability”~~ column. ~~The “Applicable Systems” column to~~ further defines the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R1 – Security Awareness Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R1 – Security Awareness Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004- ~~X7~~ Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

- R2.** Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-~~X7~~ *Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- M2.** Evidence must include the training program that includes each of the applicable requirement parts in CIP-004-~~X7~~ *Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~X7~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~X7~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

- R3.** Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M3.** Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R3 – Personnel Risk Assessment Program and additional evidence to demonstrate implementation of the program(s).

CIP-004- ~~X7~~ Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~X7~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004- ~~X7~~ Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004- ~~X7~~ Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

- R4.** Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R4 – Access Management Program and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004- ~~X7~~ Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and ~~2.~~ PACS ~~3.2.~~ _____	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter.

CIP-004- ~~X7~~ Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~X7~~ Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

- R5.** Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R5 – Access Revocation. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.
- M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R5 – Access Revocation and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004- ~~X7~~ Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004- ~~X7~~ Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004- ~~X7~~ Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	High Impact BES Cyber Systems and their associated: EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~X7~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.4	High Impact BES Cyber Systems and their associated: EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: - Workflow or sign-off form showing password reset within 30 calendar days of the termination; - Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or - Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

- R6.** Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to ~~for BES Cyber System Information~~ BCSI pertaining to the “Applicable Systems” identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-~~X7~~ Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M6.** Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in CIP-004-~~X7~~ Table R6 – Access Management for BES Cyber System Information and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X7 Table R6 – Access Management for BES Cyber System Information			
Part	Applicable Systems	Requirements	Measures
6.1	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	<u>Prior to provisioning, authorize (unless already authorized according to Part 4.1.) provisioning of access to BCSI based on need (unless already authorized according to Part 4.1.), as determined by the Responsible Entity, except for CIP Exceptional Circumstances:-</u> <u>6.1.1. Provisioned electronic access to electronic BCSI; and</u> <u>6.1.2 Provisioned physical access to physical BCSI.</u> <u>Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).</u>	Examples of evidence may include, but are not limited to, ~~the following:-~~ <u>individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.</u> ~~• Dated authorization records for provisioned access to BCSI based on need; or~~ ~~• List of authorized individuals~~

CIP-004-X7 Table R6 – Access Management for BES Cyber System Information			
Part	Applicable Systems	Requirements	Measures
6.2	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all <u>individuals with</u> provisioned access to BCSI: 6.2.1. <u>have an ~~is~~-authorized record</u>; and 6.2.2. <u>~~is still need the provisioned access to perform their current work functions, appropriate based on need,~~</u> as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, <u>the documentation of the review that includes</u> all of the following: • List of authorized individuals; ~~and~~ • List of individuals who have been provisioned access; ~~and~~ • ~~List of privileges associated with the authorizations; and~~ • ~~List of privileges associated with the provisioned access; and~~ • ~~Dated documentation of the 15-calendar month verification; and~~ • <u>Verification that provisioned access is appropriate based on need; and</u> • Documented reconciliation actions, if any.

CIP-004- ~~X7~~ Table R6 – Access Management for BES Cyber System Information			
Part	Applicable ~~Security~~ Systems	Requirements	Measures
6.3	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The ~~Compliance Enforcement Authority~~CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment Processes~~Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	Operations Planning	Lower	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	Operations Planning	Medium	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of	perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				previous PRA completion date. (3.5)	the previous PRA completion date. (3.5)	for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	Operations Planning and Same Day Operations	Medium	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action,	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	Same Day Operations and	Medium	<u>The Responsible Entity has implemented one or more program(s) as</u>	<u>The Responsible Entity has implemented one or more program(s) as</u>	<u>The Responsible Entity has implemented one or more program(s) as</u>	<u>The Responsible Entity did not implement one or more documented</u>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations Planning		<u>required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</u> <u>OR</u> <u>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2)</u> <u>OR</u> <u>The Responsible Entity has implemented one or more process(es) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do</u>	<u>required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</u> <u>OR</u> <u>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2)</u> <u>OR</u> <u>The Responsible Entity has implemented one or more process(es) to remove the individual's ability to use</u>	<u>required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</u> <u>OR</u> <u>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2)</u> <u>OR</u> <u>The Responsible Entity has implemented one or more process(es) to remove the individual's ability to</u>	<u>access management program(s) for BCSI. (R6)</u> <u>OR</u> <u>The Responsible Entity has implemented one or more process(es) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</u> <u>OR</u> <u>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2)</u> <u>OR</u>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- ~~X7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>so by the timeframe required in Requirement R6, Part 6.3.</u> ~~The Responsible Entity has implemented one or more documented access management program(s) for BCSI but did not implement one of the applicable items for Parts 6.1 through 6.3. (R6)~~	<u>provisioned access to BCSI but, for two individuals, did not do so by timeframe required in Requirement R6, Part 6.3.</u> ~~The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement two of the applicable items for Parts 6.1 through 6.3 (R6)~~	<u>use provisioned access to BCSI but, for three individuals, did not do so by timeframe required in Requirement R6, Part 6.3.</u> ~~The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement three of the applicable items for Parts 6.1 through 6.3 (R6)~~	<u>The Responsible Entity has implemented one or more process(es) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by timeframe required in Requirement R6, Part 6.3.</u> ~~The Responsible Entity did not implement one or more documented access management program(s) for BCSI (R6)~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to

Version	Date	Action	Change Tracking
			revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSl.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
<u>45-day formal comment period with ballot</u>	<u>August 6– September 21, 2020</u>
<u>45-day formal comment period with ballot</u>	<u>March 25 – May 10, 2021</u>

Anticipated Actions	Date
~~45-day formal or informal comment period with ballot~~	~~August 2020~~
10-day final ballot	~~September~~ <u>May</u> 202 ~~10~~
Board adoption	November 202 ~~10~~

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-~~X3~~
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Reliability Coordinator**
 - 4.1.6 **Transmission Operator**

4.1.7 Transmission Owner

- 4.2. Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

- 4.2.1 Distribution Provider:** One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~X3~~:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-011-~~X3~~.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” ~~and “Applicability”~~ Columns in Tables:

Each table has an “Applicable Systems” ~~or “Applicability”~~ column. ~~The “Applicable Systems”~~ column to further defines the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1~~a~~ identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1~~a~~ identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to “Applicable Systems” identified in CIP-011-X Table R1 – Information Protection Program that collectively includes each of the applicable requirement parts in CIP-011-~~X3~~ Table R1 – Information Protection Program. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.
- M1.** Evidence for the information protection program must include the applicable requirement parts in CIP-011-~~X3~~ Table R1 – Information Protection Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~X3~~ Table R1 – Information Protection Program

Part	Applicable ~~le Systems~~ ~~ility~~	Requirements	Measures
1.1	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence <u>may</u> include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	~~BCSI as identified in Part 1.1~~ <u>High Impact BES Cyber Systems and their associated:</u> <u>1. EACMS; and</u> <u>2. PACS</u> <u>Medium Impact BES Cyber Systems and their associated:</u>	Method(s) to protect and securely handle BCSI <u>to mitigate risks of compromising confidentiality.</u>	Examples of acceptable evidence <u>for on-premise BCSI may</u> include, but are not limited to, the following: • <u>Procedures for protecting and securely handling BCSI, which include topics such as storage, security during transit, and use; or</u>

	<u>1. EACMS; and</u> <u>2. PACS</u>	• <u>Records indicating that</u> BCSI is handled in a manner consistent with the entity's documented procedure(s). <u>Examples of evidence for off-premise BCSI may include, but are not limited to, the following:</u> • <u>Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or</u> • <u>Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or</u> • <u>Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).</u> • ~~Evidence of methods used to protect and securely handle BCSI during its lifecycle, including:~~ • ~~Electronic mechanisms,~~ • ~~Physical mechanisms,~~

CIP-011- ~~X3~~ Table R1 – Information Protection Program			
Part	Applicable ~~le Systems~~ ~~ility~~	Requirements	Measures
			~~• Technical mechanisms, or~~ ~~• Administrative mechanisms~~

CIP-011- ~~X3~~ Table R1—Information Protection Program			
Part	Applicability	Requirement	Measure
1.3	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk identification and assessment method(s) for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.	Examples of acceptable evidence may include, but are not limited to, dated documentation of the following: • Implementation of the risk identification and assessment method(s) (1.3); • Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under layer to the service provider, including application, infrastructure, and network security controls as well as physical access controls (1.3.2, 1.3.3, 1.3.4); • Business agreements that include communication expectations and protocols for disclosures of known vulnerabilities, access breaches, incident response, transparency regarding licensing, data ownership, and metadata (1.3.1); • Consideration made for data sovereignty, if any (1.3.1);

			• ~~Considerations used to assess conversion of data from one form to another and how information is protected from creation to disposal (1.3.1, 1.3.3);~~ • ~~Dated documentation of vendor's identity and access management program (1.3.2); and~~ • ~~Physical and electronic security management documentation, (e.g., plans, diagrams) (1.3.3).~~
1.4	~~BCSI as identified in Part 1.1~~	~~When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.~~	Examples of evidence may include, but are not limited to, dated documentation of the following: • ~~Description of the electronic technical mechanism(s) (e.g., data masking, encryption, hashing, tokenization, cypher, electronic key management method[s]);~~ • ~~Evidence of implementation (e.g., configuration files, command output, architecture documents); and~~ • ~~Technical mechanism(s) for the separation of duties, demonstrating that entity's control(s) cannot be subverted by the custodial vendor.~~

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-~~X3~~ Table R2 – BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-011-~~X3~~ Table R2 – BES Cyber Asset Reuse and Disposal and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011- ~~X3~~ Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence <u>may</u> include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-~~X3~~ Table R2 – BES Cyber Asset Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI ~~BES Cyber Information~~ prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~ CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~ CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The ~~Compliance Enforcement Authority~~ CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment Processes~~ Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

2. Table of Compliance Elements

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- ~~X3~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	~~N/A The Responsible Entity implemented one or more documented information protection program(s) but did not implement one of the applicable items for Parts 1.1 through 1.4. (R1)~~	~~N/A The Responsible Entity implemented one or more documented information protection program(s) but did not implement two of the applicable items for Parts 1.1 through 1.4. (R1)~~	~~The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1)~~ ~~OR~~ ~~The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1)~~ ~~OR~~ ~~The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)~~ ~~The Responsible Entity implemented one or more~~	~~The Responsible Entity neither documented nor implemented did not implement one or more BCSI documented information protection program(s). (R1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- ~~X3~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~documented information protection program(s) but did not implement three or more of the applicable items for Parts 1.1 through 1.4. (R1)~~	
R2	Operations Planning	Lower	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011- ~~X3~~ Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents**Version History**

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSl.

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information

SAR Title:	PRC-005-6 applicability to AVR protective functions		
Date Submitted:	6/8/2020		
SAR Requester			
Name:	Brian Kasmarzik, Chair		
Organization:	Project 2019-04 Modifications to PRC-005-6 SAR Drafting Team		
Telephone:	314-554-4315	Email:	BKasmarzik@ameren.com

SAR Type (Check as many as apply)

☒ ☒ ☒ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ ☐ Revision to Existing Standard	☐ Variance development or revision
☒ ☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)

☐ Regulatory Initiation	☐ NERC Standing Committee Identified
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☒ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

PRC-005-~~6~~ will be revised to provide clarity that the BES protective functions enabled within excitation systems (including analog/digital Automatic Voltage Regulators (AVRs)), and BES protective functions enabled within other control systems, that respond to electrical quantities ~~and act to cease injecting current (75 MVA or greater) or and~~ trip BES elements either directly or via lockout or auxiliary tripping relays are within the scope of the standard. The clarity that is needed is regarding protective functions inside excitation systems and control systems which are not stand-alone relays, but otherwise perform as a BES Protection System. Without clear applicability, the industry is struggling with how to implement PRC-005 and what testing is acceptable to meet the required maintenance activities prescribed by PRC-005. The lack of clarity presents a reliability gap in the application of PRC-005.

Additionally, there are Protection System ~~Station-station~~ direct current (DC) supply technologies that do not currently have maintenance activities established in PRC-005. The standard needs to address battery-based station DC technologies that are not covered by PRC-005 and consider other emerging alternative technologies, both battery-based and non-battery-based.

Requested information
This project would modify Reliability Standard PRC-005-~~6~~ to be consistent with the Federal Energy Regulatory Commission (FERC)-approved changes to registration as part of the Risk Based Registration (RBR) initiative by specifying Underfrequency Load Shedding (UFLS)-only Distribution Providers (DPs) in the Applicability Section.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
Provide clear, unambiguous applicability of PRC-005 to protective functions and provide the specificity needed for the industry to consistently identify and implement the required maintenance activities.
Provide for the use of <u>emerging alternative</u> Protection System <u>Station-station</u> DC supply technologies, battery based and non-battery-based, and ensure that they are subject to maintenance requirements.
This project would modify Reliability Standard PRC-005-~~6~~ to be consistent with the FERC-approved changes to registration as part of the RBR initiative and to add UFLS-only DPs in the Applicability Section.
Project Scope (Define the parameters of the proposed project):
Modify PRC-005 to provide clarity that the <u>BES</u> protective functions enabled within analog/digital AVRs, excitation systems, and <u>BES protective functions enabled within</u> other control systems that respond to electrical quantities ~~and act to cease injecting current or~~ trip BES elements either directly or via lockout or auxiliary tripping relays are within the scope of the standard. Modifications to PRC-005-~~6~~ could also include defining terms, revising applicability, modifying maintenance activities and intervals, or other appropriate modifications needed to provide clarity. In addition, modify the PRC-005-~~6~~ Supplementary Reference and FAQ to align with revisions to PRC-005-~~6~~.
The clarifying changes would apply to BES Protection Systems and <u>BES</u> protective functions applied on generators, dispersed power-producing resources from the point of aggregation (greater than 75 MVA) to the point of Interconnection, static and synchronous condensers and other BES elements as defined.
Modify PRC-005-~~6~~ to establish maintenance requirements for Protection System DC supply technologies that are not currently covered.
This project would modify Reliability Standard PRC-005-~~6~~ to be consistent with the FERC-approved changes to registration as part of the RBR initiative and to add UFLS-only DPs in the Applicability Section.

Requested information

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):

The North American Generator Forum (NAGF) received feedback from members indicating that there was confusion regarding the applicability of protective functions inside synchronous generator excitation systems to PRC-005. The primary cause of confusion is the use of the NERC term "Protection System," which specifies "relays" but not the protective functions that are typically (but not always) associated with relays. Excitation systems may measure and utilize similar quantities as protective relays and may perform similar functions as protective relays applicable to PRC-005. For this reason, the SAR drafting team agrees that the aforementioned protective functions within excitation systems and other control systems need to be clearly and explicitly applicable to PRC-005.

PRC-005 will be modified to provide clarity on the inclusion of BES protective functions enabled within excitation systems (analog/digital AVR), and BES protective functions enabled within other control systems, that respond to electrical quantities and ~~act to cease injecting current~~ or trip BES elements either directly or via lockout or auxiliary tripping relays. The clarifying changes would apply to BES Protection Systems and BES protective functions applied on generators, dispersed power producing resources from the point of aggregation (greater than 75 MVA) to the point of Interconnection, static and synchronous condensers and other BES elements as defined.

The SAR drafting team recommends considering the specification of American National Standards Institute (ANSI) Standard Device Numbers for the applicability to PRC-005 as outlined in the Applicability Section 4.2. Other options to provide clarity include: developing standard-specific definitions, developing or revising existing terms in the NERC Glossary of Terms, or making other modifications to the Applicability section.

The maintenance tables should be updated to include the aforementioned BES protective functions enabled within other control systems, and the associated maintenance activities and intervals. -

Additionally, the maintenance tables should be updated to include new DC supply technologies for Protection System(s) not currently captured.

Entities registered as ULFS-Only (DPs) have PRC-005-~~6~~-applicable Protection Systems, but are not expressly listed as Applicable Entities in Section 4.1 UFLS-Only DPs should be added to the Applicability Section to avoid any confusion and to be consistent with the FERC-approved RBR registration changes.

Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information	
The SAR DT is seeking industry input regarding cost impact.	
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):	
The clarifying changes would apply to BES Protection Systems and BES protective functions applied on generators, dispersed power producing resources from the point of aggregation (greater than 75 MVA) to the point of Interconnection, static and synchronous condensers and other BES elements as defined. The items under consideration related to DC supply technologies would impact multiple facility owners.	
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):	
Generator Owner (GO), Transmission Owner (TO), Distribution Provider (DP), Underfrequency Load Shedding (UFLS)-only DP	
Do you know of any consensus building activities ² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.	
The NAGF and the NEI worked together to generate the initial SAR and communicated the issue in advance to NERC.	
This project would modify Reliability Standard PRC-005- ~~6~~ to be consistent with the FERC-approved changes to registration as part of the RBR initiative and to add UFLS-only DPs in the Applicability Section.	
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?	
Options to provide clarity for PRC-005 include: developing standard-specific definitions, developing or revising existing terms in the NERC Glossary of Terms, or making other modifications to the Applicability section. In the event of developing or revising existing terms in the NERC Glossary of Terms, review of the effects on other standards must be performed.	
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.	

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
<i>e.g.</i> , NPCC	None

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of the proposed standard for a formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR)	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
45-day initial formal comment period with ballot	January <u>27 – March 12,</u> 2021
<u>25-day formal comment period with ballot</u>	<u>April 2 – 27, 2021</u>

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~May 2021~~
~~45-day formal comment period with additional ballot~~	~~July 2021~~
10-day final ballot	~~October 1 – 11,~~ <u>May</u> 2021
NERC Board (Board) adoption	~~November~~ <u>June</u> 2021

A. Introduction

1. **Title:** Emergency Preparedness and Operations
2. **Number:** EOP-011-2
Purpose: To address the effects of operating emergencies by ensuringe each Transmission Operator, Balancing Authority, and Generator Owner has developed plan(s) to mitigate ~~and prepare for~~ operating Emergencies; and that ~~Operating those P~~plans are implemented and coordinated within ~~a the~~ Reliability Coordinator Area as specified within the requirements. Area-
3. **Applicability:**
 - 3.1. **Functional Entities:**
 - 3.1.1 Balancing Authority
 - 3.1.2 Reliability Coordinator
 - 3.1.3 Transmission Operator
 - 3.1.4 Generator Owner
 - 3.1.5 Generator Operator
 - 3.2. **Facilities**
 - 3.2.1 For the purpose of this standard, the term “generating unit” includes means all Bulk Electric System generatorsing units and BES generating plants.
4. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements and Measures

- R1. Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*
 - 1.1. Roles and responsibilities for activating the Operating Plan(s);
 - 1.2. Processes to prepare for and mitigate Emergencies including:
 - 1.2.1. Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;
 - 1.2.2. Cancellation or recall of Transmission and generation outages;
 - 1.2.3. Transmission system reconfiguration;
 - 1.2.4. Redispatch of generation request;

- 1.2.5. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and
 - 1.2.6. Provisions to determine Reliability impacts of:
 - 1.2.6.1. cold weather conditions; and
 - 1.2.6.2. ~~any other~~ extreme weather conditions.
- M1. Each Transmission Operator will have a dated Operating Plan(s) developed in accordance with Requirement R1 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R1.
- R2. Each Balancing Authority shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate Capacity Emergencies and Energy Emergencies within its Balancing Authority Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*
 - 2.1. Roles and responsibilities for activating the Operating Plan(s);
 - 2.2. Processes to prepare for and mitigate Emergencies including:
 - 2.2.1. Notification to its Reliability Coordinator, to include current and projected conditions when experiencing a Capacity Emergency or Energy Emergency;
 - 2.2.2. Requesting an Energy Emergency Alert, per Attachment 1;
 - 2.2.3. Managing generating resources in its Balancing Authority Area to address:
 - 2.2.3.1. capability and availability;
 - 2.2.3.2. fuel supply and inventory concerns;
 - 2.2.3.3. fuel switching capabilities; and
 - 2.2.3.4. environmental constraints.
 - 2.2.4. Public appeals for voluntary Load reductions;
 - 2.2.5. Requests to government agencies to implement their programs to achieve necessary energy reductions;
 - 2.2.6. Reduction of internal utility energy use;
 - 2.2.7. Use of Interruptible Load, curtailable Load and demand response;

- 2.2.8. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and
 - 2.2.9. Provisions to determine Reliability impacts of:
 - 2.2.9.1. cold weather conditions; and
 - 2.2.9.2. ~~any other~~ extreme weather conditions.
- M2. Each Balancing Authority will have a dated Operating Plan(s) developed in accordance with Requirement R2 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings, or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R2.
- R3. The Reliability Coordinator shall review the Operating Plan(s) to mitigate operating Emergencies submitted by a Transmission Operator or a Balancing Authority regarding any reliability risks that are identified between Operating Plans. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*
 - 3.1. Within 30 calendar days of receipt, the Reliability Coordinator shall:
 - 3.1.1. Review each submitted Operating Plan(s) on the basis of compatibility and inter-dependency with other Balancing Authorities' and Transmission Operators' Operating Plans;
 - 3.1.2. Review each submitted Operating Plan(s) for coordination to avoid risk to Wide Area reliability; and
 - 3.1.3. Notify each Balancing Authority and Transmission Operator of the results of its review, specifying any time frame for resubmittal of its Operating Plan(s) if revisions are identified.
- M3. The Reliability Coordinator will have documentation, such as dated e-mails or other correspondences that it reviewed Transmission Operator and Balancing Authority Operating Plans within 30 calendar days of submittal in accordance with Requirement R3.
- R4. Each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator within a time period specified by its Reliability Coordinator. *[Violation Risk Factor: High] [Time Horizon: Operation Planning]*
- M4. The Transmission Operator and Balancing Authority will have documentation, such as dated emails or other correspondence, with an Operating Plan(s) version history showing that it responded and updated the Operating Plan(s) within the timeframe identified by its Reliability Coordinator in accordance with Requirement R4.

- R5.** Each Reliability Coordinator that receives an Emergency notification from a Transmission Operator or Balancing Authority within its Reliability Coordinator Area shall notify, within 30 minutes from the time of receiving notification, other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*
- M5.** Each Reliability Coordinator that receives an Emergency notification from a Balancing Authority or Transmission Operator within its Reliability Coordinator Area will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that will be used to determine if the Reliability Coordinator communicated, in accordance with Requirement R5, with other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators .
- R6.** Each Reliability Coordinator that has a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area shall declare an Energy Emergency Alert, as detailed in Attachment 1. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*
- M6.** Each Reliability Coordinator, with a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area, will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that it declared an Energy Emergency Alert, as detailed in Attachment 1, in accordance with Requirement R6.
- R7.** Each Generator Owner shall ~~develop, implement and~~ maintain, ~~and implement~~ one or more cold weather preparedness plan(s) for its generating units. The cold weather preparedness plan(s) shall include the following, at a minimum: *[Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-Time Operations]*
- 7.1.** Generating unit(s) freeze protection measures based on ~~unique factors~~ such as geographical location and plant configuration;
- 7.2.** Annual ~~maintenance and~~ inspection and maintenance of generating unit(s) freeze protection measures;
- 7.3.** Generating unit(s) cold weather data, to include:
- 7.3.1.** Generating unit(s) operating limitations in cold weather ~~to include: 1 through 2.2. 3.4; and~~
- 7.3.1.1.** capability and availability;
- 7.3.1.2.** fuel supply and inventory concerns;
- 7.3.1.3.** fuel switching capabilities; and
- 7.3.1.4.** environmental constraints.

7.3.2. Generating unit(s):

7.3.2.1. minimum design temperature; or

7.3.2.2. minimum historical operating temperature; demonstrated historical performance during cold weather in the previous 5 years; or

7.3.2.3 engineering analysis to determine current minimum cold weather performance temperature

M7. Each Generator Owner ~~shall will~~ have evidence a document~~inged that its~~ cold weather preparedness plan(s) was implemented and maintained in accordance with Requirement R7.; ~~and have evidence such as (a review or revision history to indicate that the plan has been maintained;) and have evidence such as operator checklists, work orders, test records, other operating and maintenance documentation, or other communication documentation to show that its cold weather preparedness plan was implemented; and have evidence such as training materials and attendance list showing successful completion of training.~~

R8. Each Generator Operator or Generator Owner shall provide generating unit-specific training to its maintenance or operations personnel responsible for implementing cold weather preparedness plan(s). *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning, Operations Planning]*

M8. Each Generator Operator or Generator Owner will have documented evidence that the applicable personnel completed training of the Generator Owner's cold weather preparedness plan(s). This evidence may include, but is not limited to, documents such as personnel training records, training materials, date of training, agendas or learning objectives, attendance at pre-work briefings, review of work order tasks, tailboards, attendance logs for classroom training, and completion records for computer-based training in fulfillment of Requirement R8.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

“Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with the mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Transmission Operator shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R1 and R4 and Measures M1 and M4.
- The Balancing Authority shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R2 and R4, and Measures M2 and M4.
- The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.
- The Generator Owner shall retain the cold weather preparedness plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirement R7 and Measure M7.
- The Generator Owner or Generator Operator shall keep data or evidence to show compliance for three years or since its last compliance audit, whichever timeframe is greater, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation, for Requirement R8 and Measure M8.

1.3. Compliance Monitoring and Enforcement Program:

As defined in the NERC Rules of Procedure; “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be

used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to maintain it.	The Transmission Operator developed an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to have it reviewed by its Reliability Coordinator.	The Transmission Operator failed to develop an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. OR The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission s Operator Area but failed to implement it.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to maintain it.	The Balancing Authority developed an Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to have it reviewed by its Reliability Coordinator.	The Balancing Authority failed to develop an Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area. OR The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to implement it.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Planning	High	N/A	N/A	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator within 30 calendar days.	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator.
R4	Operations Planning	High	N/A	N/A	The Transmission Operator or Balancing Authority failed to update and resubmit its Operating Plan(s) to its Reliability Coordinator within the timeframe specified by its Reliability Coordinator.	The Transmission Operator or Balancing Authority failed to update and resubmit its Operating Plan(s) to its Reliability Coordinator.
R5	Real-time Operations	High	N/A	N/A	The Reliability Coordinator that received an Emergency	The Reliability Coordinator that received an Emergency

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					notification from a Transmission Operator or Balancing Authority did notify neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators but failed to notify within 30 minutes from the time of receiving notification.	notification from a Transmission Operator or Balancing Authority failed to notify neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators.
R6	Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator that had a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area failed to declare an Energy Emergency Alert.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	Operations Planning and Real-time Operations	High	<u>The Generator Owner implemented a cold weather preparedness plan(s) but failed to maintain it.</u> ~~The Generator Owner's cold weather preparedness plan failed to include one of the applicable requirement Parts within Requirement R7.~~	<u>The Generator Owner's cold weather preparedness plan failed to include one of the applicable requirement Parts within Requirement R7.</u> ~~The Generator Owner developed a cold weather preparedness plan(s) but failed to maintain it.~~ OR ~~The Generator Owner's cold weather preparedness plan failed to include two of the applicable requirement Parts within Requirement R7.~~	The Generator Owner ~~developed had~~ and maintained a cold weather preparedness plan(s) but failed to fully implement it. OR The Generator Owner's cold weather preparedness plan failed to include ~~three two~~ of the applicable requirement Parts within Requirement R7.	The Generator Owner does not have a cold weather preparedness plan. OR The Generator Owner has a cold weather preparedness plan, but failed to include ~~all~~ <u>any of</u> the applicable requirement Parts within Requirement R7.
R8	<u>Operations Planning and</u>	<u>Medium</u>	<u>The Generator Owner or Generator Operator failed to</u>	<u>The Generator Owner or Generator Operator failed to</u>	<u>The Generator Owner or Generator Operator failed to</u>	<u>The Generator Owner or Generator Operator failed to</u>

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	<u>Real-time Operations</u>		<u>provide generating unit-specific training as described in Requirement R8 to the greater of:</u> <u>one applicable personnel at a single generating unit; or</u> <u>5% or less of its total applicable personnel.</u>	<u>provide generating unit-specific training as described in Requirement R8 to the greater of:</u> <u>two applicable personnel at a single generating unit; or</u> <u>more than 5% or less than or equal to 10% of its total applicable personnel.</u>	<u>provide generating unit-specific training as described in Requirement R8 to the greater of:</u> <u>three applicable personnel at a single generating unit; or</u> <u>more than 10% or less than or equal to 15% of its total applicable personnel.</u>	<u>provide generating unit-specific training as described in Requirement R8 to the greater of:</u> <u>four applicable personnel at a single generating unit; or</u> <u>more than 15% of its total applicable personnel.</u>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by Board of Trustees	Merged EOP-001-2.1b, EOP-002-3.1 and EOP-003-2.
1	November 19, 2015	FERC approved EOP-011-1. Docket Nos. RM15-7-000, RM15-12-000, and RM15-13-000. Order No. 818	
2	TBD	Adopted by the Board of Trustees	Revised under Project 2019-06

Attachment 1-EOP-011-2 Energy Emergency Alerts

Introduction

This Attachment provides the process and descriptions of the levels used by the Reliability Coordinator in which it communicates the condition of a Balancing Authority which is experiencing an Energy Emergency.

A. General Responsibilities

- 1. Initiation by Reliability Coordinator.** An Energy Emergency Alert (EEA) may be initiated only by a Reliability Coordinator at 1) the Reliability Coordinator's own request, or 2) upon the request of an energy deficient Balancing Authority.
- 2. Notification.** A Reliability Coordinator who declares an EEA shall notify all Balancing Authorities and Transmission Operators in its Reliability Coordinator Area. The Reliability Coordinator shall also notify all neighboring Reliability Coordinators.

B. EEA Levels

Introduction

To ensure that all Reliability Coordinators clearly understand potential and actual Energy Emergencies in the Interconnection, NERC has established three levels of EEAs. The Reliability Coordinators will use these terms when communicating Energy Emergencies to each other. An EEA is an Emergency procedure, not a daily operating practice, and is not intended as an alternative to compliance with NERC Reliability Standards.

The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially.

1. EEA 1 — All available generation resources in use.

Circumstances:

- The Balancing Authority is experiencing conditions where all available generation resources are committed to meet firm Load, firm transactions, and reserve commitments, and is concerned about sustaining its required Contingency Reserves.
- Non-firm wholesale energy sales (other than those that are recallable to meet reserve requirements) have been curtailed.

2. EEA 2 — Load management procedures in effect.

Circumstances:

- The Balancing Authority is no longer able to provide its expected energy requirements and is an energy deficient Balancing Authority.
- An energy deficient Balancing Authority has implemented its Operating Plan(s) to mitigate Emergencies.

- An energy deficient Balancing Authority is still able to maintain minimum Contingency Reserve requirements.

During EEA 2, Reliability Coordinators and energy deficient Balancing Authorities have the following responsibilities:

2.1 Notifying other Balancing Authorities and market participants. The energy deficient Balancing Authority shall communicate its needs to other Balancing Authorities and market participants. Upon request from the energy deficient Balancing Authority, the respective Reliability Coordinator shall post the declaration of the alert level, along with the name of the energy deficient Balancing Authority on the RCIS website.

2.2 Declaration period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 2 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators.

2.3 Sharing information on resource availability. Other Reliability Coordinators of Balancing Authorities with available resources shall coordinate, as appropriate, with the Reliability Coordinator that has an energy deficient Balancing Authority.

2.4 Evaluating and mitigating Transmission limitations. The Reliability Coordinator shall review Transmission outages and work with the Transmission Operator(s) to see if it's possible to return to service any Transmission Elements that may relieve the loading on System Operating Limits (SOLs) or Interconnection Reliability Operating Limits (IROLs).

2.5 Requesting Balancing Authority actions. Before requesting an EEA 3, the energy deficient Balancing Authority must make use of all available resources; this includes, but is not limited to:

2.5.1 All available generation units are on line. All generation capable of being on line in the time frame of the Emergency is on line.

2.5.2 Demand-Side Management. Activate Demand-Side Management within provisions of any applicable agreements.

3. EEA 3 —Firm Load interruption is imminent or in progress.

Circumstances:

- The energy deficient Balancing Authority is unable to meet minimum Contingency Reserve requirements.

During EEA 3, Reliability Coordinators and Balancing Authorities have the following responsibilities:

3.1 Continue actions from EEA 2. The Reliability Coordinators and the energy deficient Balancing Authority shall continue to take all actions initiated during EEA 2.

3.2 Declaration Period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 3 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities, and Transmission Operators.

3.3 Reevaluating and revising SOLs and IROLs. The Reliability Coordinator shall evaluate the risks of revising SOLs and IROLs for the possibility of delivery of energy to the energy deficient Balancing Authority. Reevaluation of SOLs and IROLs shall be coordinated with other Reliability Coordinators and only with the agreement of the Transmission Operator whose Transmission Owner (TO) equipment would be affected. SOLs and IROLs shall only be revised as long as an EEA 3 condition exists, or as allowed by the Transmission Owner whose equipment is at risk. The following are minimum requirements that must be met before SOLs or IROLs are revised:

3.3.1 Energy deficient Balancing Authority obligations. The energy deficient Balancing Authority, upon notification from its Reliability Coordinator of the situation, it will immediately take whatever actions are necessary to mitigate any undue risk to the Interconnection. These actions may include Load shedding.

3.4 Returning to pre-Emergency conditions. Whenever energy is made available to an energy deficient Balancing Authority such that the Systems can be returned to its pre-Emergency SOLs or IROLs condition, the energy deficient Balancing Authority shall request the Reliability Coordinator to downgrade the alert level.

3.4.1 Notification of other parties. Upon notification from the energy deficient Balancing Authority that an alert has been downgraded, the Reliability Coordinator shall notify the neighboring Reliability Coordinators (via the RCIS), Balancing Authorities and Transmission Operators that its Systems can be returned to its normal limits.

Alert 0 - Termination. When the energy deficient Balancing Authority is able to meet its Load and Operating Reserve requirements, it shall request its Reliability Coordinator to terminate the EEA.

3.4.2 Notification. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS of the termination. The Reliability Coordinator shall also notify the neighboring Balancing Authorities and Transmission Operators.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of proposed standard for formal a 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR) for posting	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
<u>45-day initial formal comment period with ballot</u>	<u>January 27 – March 12, 2021</u>
<u>25-day initial formal comment period with ballot</u>	<u>April 2 – April 27, 2021</u>

Anticipated Actions	Date
~~45-day initial formal comment period with ballot~~	~~January 2021~~
~~45-day formal comment period with ballot~~	~~May 2021~~
~~45-day formal comment period with additional ballot~~	~~July 2021~~
10-day final ballot	~~October 1~~ <u>May 11</u> , 2021
NERC Board (Board) adoption	~~November~~ <u>June 11</u> , 2021

A. Introduction

1. **Title:** Reliability Coordinator Data Specification and Collection
2. **Number:** IRO-010-~~54~~
3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring the Reliability Coordinator has the data it needs to monitor and assess the operation of its Reliability Coordinator Area.
4. **Applicability**
 - 4.1. Reliability Coordinator~~;~~
 - 4.2. Balancing Authority~~;~~
 - 4.3. Generator Owner~~;~~
 - 4.4. Generator Operator~~;~~
 - 4.5. Transmission Operator~~;~~
 - 4.6. Transmission Owner~~;~~
 - 4.7. Distribution Provider~~;~~
5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements

- R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to: *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*
 - 1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.
 - 1.2. Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.
 - 1.3. Provisions for notification of BES generating unit~~(s)~~ ~~-specific design specification or minimum historical performance~~ during local forecasted cold weather ~~to include: ,and expected BES generating unit operation limitations during local forecasted cold weather.~~
 - 1.3.1 Operating limitations based on:
 - 1.3.1.1. capability and availability;
 - 1.3.1.2. fuel supply and inventory concerns;
 - 1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints

1.3.2. Generating unit(s):

2.3.2.1. minimum design temperature; or

2.3.2.2. minimum historical operating temperature; or

2.3.2.3. engineering analysis to determine current minimum cold weather performance temperature.

1.4. A periodicity for providing data.

1.5. The deadline by which the respondent is to provide the indicated data.

- M1.** The Reliability Coordinator shall make available its dated, current, in force documented specification for data.
- R2.** The Reliability Coordinator shall distribute its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. (*Violation Risk Factor: Low*) (*Time Horizon: Operations Planning*)
- M2.** The Reliability Coordinator shall make available evidence that it has distributed its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. This evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.
- R3.** Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall satisfy the obligations of the documented specifications using: (*Violation Risk Factor: Medium*) (*Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations*)
- 3.1.** A mutually agreeable format
- 3.2.** A mutually agreeable process for resolving data conflicts
- 3.3.** A mutually agreeable security protocol
- M3.** The Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Reliability Coordinator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall make available evidence that it satisfied the obligations of the documented specification using the specified criteria. Such evidence could include but is not limited to electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with the mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The Reliability Coordinator shall retain its dated, current, in force documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R1, Measure M1 as well as any documents in force since the last compliance audit.

The Reliability Coordinator shall keep evidence for three calendar years that it has distributed its data specification to entities that have data required by the Reliability Coordinator’s Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R2, Measure M2.

Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R3 and Measurement M3.

1.3. Compliance Monitoring and Enforcement Program:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. ~~Additional Compliance Information: None.~~

Violation Severity Levels

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R1	Operations Planning	Low	The Reliability Coordinator did not include two or fewer of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Reliability Coordinator did not have a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
						monitoring, and Real-time Assessments.
For the Requirement R2 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R2	Operations Planning	Low	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, and Real-time monitoring, and	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to four or more entities, or more than 15% of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
				Real-time Assessments.	Real-time Assessments.	Real-time Assessments.
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow one of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow two of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow any of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

None

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	Order issued by FERC approving IRO-010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	April 2014	Revisions pursuant to Project 2014-03	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC approved IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
3	October 30, 2020	FERC approved IRO-010-2. Docket No. RD20-4-000	
4	TBD	Adopted by NERC Board of Trustees	Revisions under Project 2019-06

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR)	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
45-day initial formal comment period with ballot	January <u>27 – March 12,</u> 2021
<u>25-day formal comment period with ballot</u>	<u>April 2 – 27, 2021</u>

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	May 2021
~~45-day formal comment period with additional ballot~~	~~July 2021~~
10-day final ballot	~~October 1 – 11,~~ <u>May</u> 2021
NERC Board (Board) adoption	~~November-June~~ 2021

A. Introduction

1. **Title:** Operational Reliability Data
2. **Number:** TOP-003-5
3. **Purpose:** To ensure that the Transmission Operator and Balancing Authority have data needed to fulfill their operational and planning responsibilities.
4. **Applicability:**
 - 4.1. Transmission Operator
 - 4.2. Balancing Authority
 - 4.3. Generator Owner
 - 4.4. Generator Operator
 - 4.5. Transmission Owner
 - 4.6. Distribution Provider
5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements and Measures

- R1. Each Transmission Operator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include, but not be limited to:
[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
 - 1.1. A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data as deemed necessary by the Transmission Operator.
 - 1.2. Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.
 - 1.3. Provisions for notification of BES generating unit(s) ~~specific design specification or minimum historical performance during cold weather, and expected BES generating unit operation limitations~~ during local forecasted cold weather to include:-
 - 1.3.1. Operating limitations based on:
 - 1.3.1.1. capability and availability;
 - 1.3.1.2. fuel supply and inventory concerns;
 - 1.3.1.3. fuel switching capabilities; and
 - 1.3.1.4. environmental constraints
 - 1.3.2. Generating unit(s):

1.3.2.1 minimum design temperature; or

1.3.2.2. minimum historical operating temperature; or

1.3.2.3 engineering analysis to determine current minimum cold weather performance temperature

~~1.34.~~ A periodicity for providing data.

~~1.45.~~ The deadline by which the respondent is to provide the indicated data.

M1. Each Transmission Operator shall make available its dated, current, in force documented specification for data.

R2. Each Balancing Authority shall maintain a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. A list of data and information needed by the Balancing Authority to support its analysis functions and Real-time monitoring.

2.2. Provisions for notification of current Protection System and Remedial Action Scheme status or degradation that impacts System reliability.

~~2.3.~~ ~~A periodicity for providing data.~~ Provisions for notification of BES generating unit(s) status during local forecasted cold weather to include:

2.3.1. Operating limitations based on:

2.3.1.1. capability and availability;

2.3.1.2. fuel supply and inventory concerns;

2.3.1.3. fuel switching capabilities; and

2.3.1.4. environmental constraints.

2.3.2. Generating unit(s):

2.3.2.1 minimum design temperature; or

2.3.2.2. minimum historical operating temperature; or

2.3.2.3 engineering analysis to determine current minimum cold weather performance temperature.

~~2.2.2.4.~~ A periodicity for providing data.

~~2.3.2.5.~~ The deadline by which the respondent is to provide the indicated data.

M2. Each Balancing Authority shall make available its dated, current, in force documented specification for data.

- R3.** Each Transmission Operator shall distribute its data specification to entities that have data required by the Transmission Operator’s Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- M3.** Each Transmission Operator shall make available evidence that it has distributed its data specification to entities that have data required by the Transmission Operator’s Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.
- R4.** Each Balancing Authority shall distribute its data specification to entities that have data required by the Balancing Authority’s analysis functions and Real-time monitoring. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- M4.** Each Balancing Authority shall make available evidence that it has distributed its data specification to entities that have data required by the Balancing Authority’s analysis functions and Real-time monitoring. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, or e-mail records.
- R5.** Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall satisfy the obligations of the documented specifications using: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*
- 5.1.** A mutually agreeable format
 - 5.2.** A mutually agreeable process for resolving data conflicts
 - 5.3.** A mutually agreeable security protocol
- M5.** Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall make available evidence that it has satisfied the obligations of the documented specifications. Such evidence could include, but is not limited to, electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each responsible entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

Each Transmission Operator shall retain its dated, current, in force, documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.

Each Balancing Authority shall retain its dated, current, in force, documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring in accordance with Requirement R2 and Measurement M2 as well as any documents in force since the last compliance audit.

Each Transmission Operator shall retain evidence for three calendar years that it has distributed its data specification to entities that have data required by the Transmission Operator’s Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R3 and Measurement M3.

Each Balancing Authority shall retain evidence for three calendar years that it has distributed its data specification to entities that have data required by the Balancing Authority’s analysis functions and Real-time monitoring in accordance with Requirement R4 and Measurement M4.

Each Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R5 and Measurement M5.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

~~1.4. Additional Compliance Information~~
~~None.~~

~~Table of Compliance Elements~~ Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Transmission Operator did not include two or fewer of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Transmission Operator did not have a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	Lower	The Balancing Authority did not include ~~one-two~~ or <u>fewer</u> of the parts (Part 2.1 through Part 2.45) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include ~~two-three~~ of the parts (Part 2.1 through Part 2.45) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include ~~three-four~~ of the parts (Part 2.1 through Part 2.45) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include ~~four-any~~ of the parts (Part 2.1 through Part 2.45) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. OR, The Balancing Authority did not have a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.
For the Requirement R3 and R4 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R3	Operations Planning	Lower	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specification to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to four or more entities, or more than 15% of the entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R4	Operations Planning	Lower	The Balancing Authority did not distribute its data specification to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to two entities, or more than 5% and less than or equal to 10% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to three entities, or more than 10% and less than or equal to 15% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to four or more entities, or more than 15% of the entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet one of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet two of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet three of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1		Modified R1.2 Modified M1 Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs)	Revised
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving TOP-003-1 (approval effective 5/23/11)	
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	April 2014	Changes pursuant to Project 2014-03	Revised
3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-003-3. Docket No. RM15-16-000, Order No. 817	
4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:		Revise the Applicable Facilities of MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 Standards to comprehensively include all types of dynamic reactive resources (including static var systems and FACTS) and DC transmission systems used to provide Essential Reliability Services in the Bulk Electric System.	
Date Submitted:		February 24, 2020	
SAR Requester			
Name:		Hari Singh – Chair, System Analysis & Modeling Subcommittee (SAMS)	
Organization:		Xcel Energy	
Telephone:		303-571-7095	Email: hari.singh@xcelenergy.com
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☒ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Dynamic reactive resources used to provide Essential Reliability Services (ERS) in the BES include generation resources (rotating machine and inverter-based) as well as transmission connected dynamic reactive resources (power-electronics based). Existing reliability standards for verifying the capability, modeling and performance of dynamic reactive resources are only applicable to Facilities comprising generation resources. Augmenting the applicability of these standards to include (non-generation) transmission-connected reactive resources – both rotating machine (i.e. synchronous condenser) and power-electronics based – will enhance the BES reliability by ensuring that the capability, models and performance is verified and validated for all varieties of dynamic reactive resources utilized in providing ERS in the BES.			

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
Augment the “Applicability – Facilities” and “Applicability-Functional Entities” sections in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards to address (non-generation) transmission-connected dynamic reactive resources – both rotating machine (i.e. synchronous condenser) and power-electronics based. Also modify Requirements (including applicable attachments) as needed to ensure they continue to address the additional Facilities. As needed, also define new Glossary Terms for all or some of the transmission-connected dynamic reactive devices noted in the SAMS white-paper “ <i>Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards</i> ”.
Project Scope (Define the parameters of the proposed project):
Revise the “Applicability – Facilities” section, “Applicability – Functional Entities” section, and Requirements (including applicable attachments) as needed in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards to comprehensively address all varieties of transmission-connected dynamic reactive resources that are utilized in providing ERS in the BES.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification ¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g. research paper) to guide development of the Standard or definition):
The “Applicability – Facilities” and “Applicability-Functional Entities” sections in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards will be revised to address (non-generation) transmission-connected dynamic reactive resources based on the recommendations summarized in Table 1 of the SAMS white-paper “ <i>Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards</i> ”. The white-paper also provides the technical justifications for the recommended revisions and the associated reliability benefits. Also modify Requirements (including applicable attachments) as needed to ensure they continue to address the additional Facilities. As needed, also define new Glossary Terms for all or some of the transmission-connected dynamic reactive devices noted as items 1.a – 1.j in the Additional Considerations section of the SAMS white-paper.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Unknown
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g. Dispersed Generation Resources):
Power-electronics based transmission-connected reactive resources – also known as FACTS (Flexible AC Transmission System) devices – such as: Static Var Compensator (SVC), Static Synchronous Compensator (STATCOM), HVDC Links (LCC or VSC).
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g. Transmission

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Transmission Owners in addition to the existing Functional Entities
Do you know of any consensus building activities ² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
<i>"Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards"</i> white-paper approved by SAMS members.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?
PRC-019 SAR requested by SPCS and PRC-024 SAR requested by IRPTF
Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
No viable alternatives were found by SAMS.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
<i>e.g.</i> NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☒ Draft SAR reviewed by NERC Staff ☒ Draft SAR presented to SC for acceptance ☒ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:		Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security	
Date Submitted:		March 4, 2020	
SAR Requester			
Name:		Soo Jin Kim, Senior Manager of Standards Development	
Organization:		NERC	
Telephone:		404.831.4765	Email: Soo.jin.kim@nerc.net
SAR Type (Check as many as apply)			
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)		
☒ Revision to Existing Standard	☐ Variance development or revision		
☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)		
☐ Withdraw/retire an Existing Standard			
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation	☐ NERC Standing Committee Identified		
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated		
☐ Reliability Standard Development Plan	☐ Industry Stakeholder Identified		
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The project will increase reliability through consistent supply chain protections to low impact BES Cyber Systems. The NERC Supply Chain Risk Assessment Report (December 2019) found that 87% of all BES Cyber Asset locations have low impact BES Cyber Systems, and many of these locations have external connectivity. Currently the systems at these locations would not be subject to the current Supply Chain Standards, CIP-005-6, CIP-010-3 and CIP-013-1. The impact to the reliability of the BES could be significant if multiple owners and operators allow ~~third-party~~ vendor access to their facilities and the associated BES Cyber Systems possess a common supply chain vulnerability. This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
This project will address the NERC Board resolution adopted at its February 2020 to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect			

Requested information
known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Project Scope (Define the parameters of the proposed project):
This project will address recommendations ~~form from~~ the NERC Board resolution from February 2020 Supply Chain Risk Assessment Report . This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to NERC Glossary of Terms definitions or standards and requirements.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification ¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):
Revise CIP-003-8 to include policies for low impact BES Cyber Systems at locations that allow ~~3rd~~ party vendor remote access to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Distribution Provider, Generator Owner, Generator Operator
Do you know of any consensus building activities ² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information
Project 2016-02 Modifications to CIP Standards for changes to definitions, standards or requirements. Project 2019-02 BES Cyber Systems Information Access Management for changes to definitions, standards or requirements.
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None at this time.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances

Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).

☐ Draft SAR reviewed by NERC Staff	☐ Final SAR endorsed by the SC
☐ Draft SAR presented to SC for acceptance	☐ SAR assigned a Standards Project by NERC
☐ DRAFT SAR approved for posting by the SC	☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial 45-day formal comment period with ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	03/18/20
SAR posted for comment	04/08/20

Anticipated Actions	Date
45-day formal comment period with ballot	04/26/21
10-day final ballot	July 2021
Board adoption	August 2021

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers
2. **Number:** CIP-012-~~12~~
3. **Purpose:** To protect the confidentiality, availability and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
4. **Applicability:**
 - 4.1. **Functional Entities:** The requirements in this standard apply to the following functional entities, referred to as “Responsible Entities,” that own or operate a Control Center.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Generator Operator**
 - 4.1.3. **Generator Owner**
 - 4.1.4. **Reliability Coordinator**
 - 4.1.5. **Transmission Operator**
 - 4.1.6. **Transmission Owner**
 - 4.2. **Exemptions:** The following are exempt from Reliability Standard CIP-012-~~12~~:
 - 4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
 - 4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
 - 4.2.3. A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.
5. **Effective Date:** See Implementation Plan for CIP-012-~~12~~.

B. Requirements and Measures

- R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include:
[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

- 1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;
- 1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
- 1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

R2. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to provide for the availability of communications links and data used for Real-time Assessment and Real-time monitoring while being transmitted between Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

2.1. Identification of how the Responsible Entity has provided for the availability of communications links and data used for Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;

2.2. Identification of how the Responsible Entity has addressed communications and data flow restoration to maintain continuity of operations in the Responsible Entity's plan; and

2.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for providing availability of communications links and data used for Real-time Assessment and Real-time monitoring while being transmitted between Control Centers.

M2. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R2 and documentation demonstrating the implementation of the plan(s).

B.C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.
<u>R2.</u>	<u>N/A</u>	<u>The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R2.</u>	<u>The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R2</u>	<u>The Responsible Entity failed to document plan(s) for Requirement R2;</u> <u>Or</u> <u>The Responsible Entity failed to implement any Part of its plan(s) for Requirement R2, except under CIP Exceptional Circumstances.</u>

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan.
 - Technical Rationale for CIP-012-2.
-

Version History

Version	Date	Action	Change Tracking
1		Respond to FERC Order No. 822	New
1	August 16, 2018	Adopted by NERC Board of Trustees	
1	January 23, 2020	FERC Order issued approving CIP-012-1. Docket No. RM18-20-000;	
<u>2</u>	<u>TBD</u>	<u>Adopted by NERC Board of Trustees</u>	

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	FAC-001-3 Facility Interconnection Requirements; FAC-002-2, Facility Interconnection Studies		
Date Submitted:	June 10, 2020		
SAR Requester			
Name:	Allen Shriver, Chair Jeffery Billo, Vice Chair		
Organization:	Inverter-Based Resource Performance Task Force (IRPTF)		
Telephone:	Allen: 561-904-3234 Jeffery: 512-248-6334	Email:	Allen.Shriver@NextEraEnergy.com Jeff.Billo@ercot.com
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The NERC Inverter-based Resource Performance Task Force (IRPTF) undertook an effort to perform a comprehensive review of all NERC Reliability Standards to determine if there were any potential gaps or improvements based on the work and findings of the IRPTF. The IRPTF identified several issues as part of this effort and documented its findings and recommendations in a white paper. The "IRPTF Review of NERC Reliability Standards White Paper" was approved by the Operating Committee and the Planning Committee in March 2020. Among the findings noted in the white paper, the IRPTF identified issues with FAC-001-3 and FAC-002-2 that should be addressed. The purpose of FAC-001-3 is to ensure that Facility interconnection requirements exist for Transmission Owners and Generator Owners when connecting new or materially modified facilities. The purpose of FAC-002-2 is to ensure studies are performed to analyze the impact of interconnecting new or materially			

Requested information
modified facilities on the Bulk Electric System (BES). An ambiguity exists in these standards in regards to the term “materially modified” and which entity is responsible for making such a determination. Hence, these standards need to be modified to address this issue.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
This SAR proposes to revise FAC-001-3 and FAC-002-2 to clarify requirements related to material modifications of Facilities.
Project Scope (Define the parameters of the proposed project):
The proposed scope of this project is as follows: a. Consider ways to clarify which entity is responsible for making the determination of what is considered to be a material modification to a Facility. b. Consider requiring Facility owners to notify affected entities when making a material modification to a Facility. c. Consider changing the term “materially modifying” to avoid confusion with similar terminology that is used for a different purpose in the FERC Open Access Transmission Tariff. d. Consider other manners in which to clarify existing requirements to ensure new or materially modified Facilities on the Bulk Electric System (BES) are adequately accounted for to ensure reliability.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification ¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):
Both FAC-001-3 and FAC-002-2 imply that the term “materially modified” should be used to distinguish between facility changes that are required to be studied and those that need not be studied. However, there is not a requirement for any entity to determine what changes are to be considered materially modifying and Facility owners are not required to notify potentially affected entities of these changes. This has led to confusion and potential reliability issues within industry. For example, a Transmission Planner may consider an inverter-based resource (IBR) control system software change to be materially modifying, but if the Generator Owner does not consider such a change to be materially modifying they will not notify the Transmission Planner of the change. While the existing standards do require coordination and cooperation between a Facility owner and the Transmission Planner or Planning Coordinator when a new or materially modified interconnection Facility is connected to their system, for example FAC-002-2 Requirement R5, neither standard specifies what entity is responsible for determining what is considered to be a material modification. Further, the existing language is unclear about whether these requirements only apply when a different entity is proposing to interconnect to a Facility owner’s Facility or if they also apply to the Facility owner’s new or modified Facility.

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
Additionally, in FERC-jurisdictional areas, the term “Materially Modification” refers to a new generation project’s impact on other generators in the interconnection queue. This has led to widespread confusion across the industry regarding the correct application of these terms related to the FERC Open Access Transmission Tariff (OATT) implementation and the NERC Reliability Standards requirements. The application of these terms is different between the FERC process and the NERC Reliability Standards (specifically FAC-001-3 and FAC-002-2). For example, if a Generator Owner changes out the inverters on an existing solar PV resource, the change may have no impact on other generators in the interconnection queue, and thus would not be considered a Material Modification under the FERC OATT rules. But such a change could have reliability impacts on the system that should be studied in accordance with FAC-002-2. The Standards Drafting Team should consider changing the term to avoid this confusion. FAC-001-3 and FAC-002-2 should be modified to clarify the use of “materially modifying”, particularly as it relates to compliance with the standards.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The SAR proposes to clarify and address gaps in the requirements in FAC-001-3 and FAC-002-2. The cost impact is unknown.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):
The frequency of change of components could be higher for IBRs and the magnitude of such changes could vary. For example, due to a rapid change in wind turbine generator (WTG) technology, it is a common practice to re-power an existing wind power plant with bigger blades while keeping the same electrical generator and converter systems (for both Type 3 and Type 4 WTGs). This may be considered a material modification since a new set of bigger blades (e.g., 93 m to 208 m) can produce more power at a lower wind speed. However, the nameplate rating of the plant will remain unchanged. From an interconnection requirements’ perspective, it is the electrical generator and converter system that impacts the majority of the steady-state, short-circuit, and dynamic characteristics and therefore will be mostly unchanged. Therefore, the question remains if these sort of repowering projects should be studied under FAC-002-2 R1 and which entity should make that determination.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Planning Coordinator, Transmission Planner, Generator Owner, Transmission Owner, Distribution Provider
Do you know of any consensus building activities² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This issue was captured in the “IRPTF Review of NERC Reliability Standards White Paper” which was approved by the Operating Committee and the Planning Committee.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
N/A
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
The IRPTF did not identify any alternatives since there are ambiguities in the existing language for FAC-001-3 and FAC-002-2 that need to be clarified.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances

Region(s)/ Interconnection	Explanation
None	N/A

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).

☐ Draft SAR reviewed by NERC Staff	☐ Final SAR endorsed by the SC
☐ Draft SAR presented to SC for acceptance	☐ SAR assigned a Standards Project by NERC
☐ DRAFT SAR approved for posting by the SC	☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:		Revise the Applicable Facilities of MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 Standards to comprehensively include all types of dynamic reactive resources (including static var systems and FACTS) and DC transmission systems used to provide Essential Reliability Services in the Bulk Electric System.	
Date Submitted:		February 24, 2020	
SAR Requester			
Name:		Hari Singh – Chair, System Analysis & Modeling Subcommittee (SAMS)	
Organization:		Xcel Energy	
Telephone:		303-571-7095	Email: hari.singh@xcelenergy.com
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☒ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Dynamic reactive resources used to provide Essential Reliability Services (ERS) in the BES include generation resources (rotating machine and inverter-based) as well as transmission connected dynamic reactive resources (power-electronics based). Existing reliability standards for verifying the capability, modeling and performance of dynamic reactive resources are only applicable to Facilities comprising generation resources. Augmenting the applicability of these standards to include (non-generation) transmission-connected reactive resources – both rotating machine (i.e. synchronous condenser) and power-electronics based – will enhance the BES reliability by ensuring that the capability, models and performance is verified and validated for all varieties of dynamic reactive resources utilized in providing ERS in the BES.			

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
Augment the “Applicability – Facilities” and “Applicability-Functional Entities” sections in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards to address (non-generation) transmission-connected dynamic reactive resources – both rotating machine (i.e. synchronous condenser) and power-electronics based. Also modify Requirements (including applicable attachments) as needed to ensure they continue to address the additional Facilities. As needed, also define new Glossary Terms for all or some of the transmission-connected dynamic reactive devices noted in the SAMS white-paper “ <i>Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards</i> ”.
Project Scope (Define the parameters of the proposed project):
Revise the “Applicability – Facilities” section, “Applicability – Functional Entities” section, and Requirements (including applicable attachments) as needed in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards to comprehensively address all varieties of transmission-connected dynamic reactive resources that are utilized in providing ERS in the BES.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification ¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g. research paper) to guide development of the Standard or definition):
The “Applicability – Facilities” and “Applicability-Functional Entities” sections in MOD-025, MOD-026, MOD-027, PRC-019 and PRC-024 reliability standards will be revised to address (non-generation) transmission-connected dynamic reactive resources based on the recommendations summarized in Table 1 of the SAMS white-paper “ <i>Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards</i> ”. The white-paper also provides the technical justifications for the recommended revisions and the associated reliability benefits. Also modify Requirements (including applicable attachments) as needed to ensure they continue to address the additional Facilities. As needed, also define new Glossary Terms for all or some of the transmission-connected dynamic reactive devices noted as items 1.a – 1.j in the Additional Considerations section of the SAMS white-paper.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Unknown
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g. Dispersed Generation Resources):
Power-electronics based transmission-connected reactive resources – also known as FACTS (Flexible AC Transmission System) devices – such as: Static Var Compensator (SVC), Static Synchronous Compensator (STATCOM), HVDC Links (LCC or VSC).
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g. Transmission

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Transmission Owners in addition to the existing Functional Entities
Do you know of any consensus building activities ² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
<i>"Transmission Connected Dynamic Reactive Resources – Assessment of Applicability in Reliability Standards"</i> white-paper approved by SAMS members.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?
PRC-019 SAR requested by SPCS and PRC-024 SAR requested by IRPTF
Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
No viable alternatives were found by SAMS.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
<i>e.g.</i> NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☒ Draft SAR reviewed by NERC Staff ☒ Draft SAR presented to SC for acceptance ☒ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	MOD-025-2 Verification and Data Reporting of Generator Capability		
Date Submitted:	10/19/2020		
SAR Requester			
Name:	Shawn Patterson, Chair		
Organization:	NERC Power Plant Modeling Verification Task Force (PPMVTF)		
Telephone:	303-445-2311	Email:	spatterson@usbr.gov
SAR Type (Check as many as apply)			
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)		
☒ Revision to Existing Standard	☐ Variance development or revision		
☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)		
☐ Withdraw/retire an Existing Standard			
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation	☒ NERC Standing Committee Identified		
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated		
☐ Reliability Standard Development Plan	☐ Industry Stakeholder Identified		
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The current industry need for this standards project is that industry implementation of MOD-025-2 has not resulted in useful unit capability data being provided for planning models of generating resources and synchronous condensers (i.e., the purpose statement of the standard). The primary reliability benefit of this project will be to correct these issues such that suitable and accurate data can be established through the verification activities performed by respective equipment owners. BPS planning assessments rely on accurate data, including machine active and reactive power capability, to identify potential reliability risks and develop mitigating actions for those risks. The current MOD-025-2 verification testing activities require significant time, expertise, and coordination; however, they do not result in data that should be used by planners for modeling purposes. The current standard does allow for optional calculations to be performed to help facilitate better information sharing; however, calculations are not required nor can be used in many cases when auxiliary equipment limits or system operating conditions prohibit reaching the actual machine capability or limiters. This standards project will address these issues.			

Requested information

Other benefits of this standards project to address issues with MOD-025-2 include, but are not limited to, the following:

- Preventing over- or under-estimation of generating facility active and reactive power, which could lead to potential reliability risks or unnecessary and expensive solutions to mitigate
- Identifying limitations within a generating facility that could constrain the resource from reaching the expected active/reactive capability at any given time
- More clearly communicating the necessary data to be used for modeling the respective resources in steady-state power flow models
- Ensure that the data users are part of the verification process to ensure that the necessary and usable data is provided and utilized appropriately
- Ensure that raw test data alone is not used for resource modeling, but is analyzed, adjusted, and contextualized to account for measured system conditions
- Coordinating with PRC-019 activities to develop a composite capability curve, inclusive of equipment capabilities, limiters, and other plant limitations to develop an appropriate capability curve
- Ensuring that other means of verification (other than testing) can be more effectively leveraged to gather necessary and suitable data for verifying plant/machine capability

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

The intent of this standard revision project is to address the issues that exist with MOD-025-2 regarding verification and data reporting of generator active and reactive power capability (and any other relevant equipment capability). Currently, implementation of the standard rarely produces data that is suitable for planning models (i.e., the stated purpose of the standard). The vast majority of testing cases are limited by limits within the plant or system operating conditions that prohibit the generating resource from reaching its “composite capability curve” – the equipment capability or associated limiters. The goal of the proposed project is to:

- Ensure that testing and other verification activities produce useful data for verification of plant active and reactive power capability
- Ensure that the data is used by Transmission Planners and Planning Coordinators in an appropriate manner, with a sufficient degree of analysis prior to use
- Ensure that the data is applicable and usable by the Transmission Planner and Planning Coordinator for reliability studies
- Ensure Generator Owners appropriately identify limits within their generating resources (and synchronous condensers), and effectively communicate those limits to Transmission Planners and Planning Coordinators for the purposes of modeling these resources in reliability studies

Requested information

Project Scope (Define the parameters of the proposed project):

The scope of this project is to modify MOD-025-2 to ensure that data provided through verification activities performed by applicable Generator Owner or Transmission Owners produce suitable data for the purposes of developing accurate planning models in Transmission Planner and Planning Coordinator reliability studies. The project should consider, at a minimum, the following:

1. Revisions to MOD-025-2 to ensure that verification activities produce data and information that can be used by Transmission Planners and Planning Coordinators for the purposes of developing accurate and reasonable plant active and reactive capability data (including possibly representation of the “composite capability curve” inclusive of capability and limiters, where applicable).
2. Ensure that each Planning Coordinator and the area Transmission Planners develop requirements for the Planning Coordinator area real and reactive capability data verification
3. Ensure that Generator Owners provide the data specified by the Planning Coordinator and Transmission Planners for the Planning Coordinator area
4. Ensure that verification activities can apply other methods beyond only testing (or real-time data) that allow plant capability information, protection settings, PRC-019 reports, and other documentation to also complement the verification activities
5. Ensure that data provided by the applicable Generator Owners and Transmission Owners is analyzed and used appropriately by Transmission Planners and Planning Coordinators
6. Ensure that the data provided by Generator Owners, if different from tested values, is acceptable to the Planning Coordinator and Transmission Planners with the standard providing guidance on acceptable reactive capability reporting if system conditions prevent reaching actual capability.
7. Ensure alignment of the MOD-025 standard with MOD-032-1 regarding data submittals for annual case creation and PRC-019-2 regarding collection of information that can be effectively used for verification purposes. Ensure activities across standards can be applied to effectively meet the purpose of these standards, and avoid any potential overlap or duplication of activities. This is dependent on the success of bullet number 1.
8. Ensure that equipment limitations are documented and classified as expected (e.g., system voltage limit reached) or unexpected (e.g., plant tripped or excitation limiter reached unexpectedly). In cases of unexpected limitations reached, ensure that the equipment owner develops and implements a corrective action plan to address this unexpected limitation.

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition): The NERC PPMVTF developed <i>White Paper: Implementation of NERC Standard MOD-025-2</i>² that recommends NERC initiate a standards project to address these issues with MOD-025-2. The white paper provides a detailed description and technical justification of the gaps that exist in MOD-025-2 and how the current standard may be leading to inaccurate data being used in BPS reliability studies. Further, the NERC PPMVTF <i>Reliability Guideline: Power Plant Model Verification and Testing for Synchronous Machines</i>³ also describes in detail how testing activities per MOD-025-2 can lead to unusable data, and provides further guidance that a SDT could use to develop solutions to these issues.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project): The aforementioned NERC PPMVTF <i>White Paper: Implementation of NERC Standard MOD-025-2</i> includes an example of one Registered Entity's MOD-025 implementation costs (excluding cost of shifting the optimization of generation fleet assets due to minimum load testing requirements). The entity's average test cost was \$1,259 (897 tests) and \$4,326 per generator (261 generators). The verification testing of units generally results in transferring energy to a higher cost resource during the test period. Further, the data produced is often NOT suitable for planning studies, which does not serve the intended purpose of the standard and makes the added cost unjustified.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources): The current MOD-025-2 was written around synchronous generation, although it is not specifically applicable only to synchronous generators. Therefore, the project should ensure the language is clear and concise regarding how to handle BES dispersed generating resources (e.g., wind, solar photovoltaic, and battery energy storage systems).
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions): Generator Owner and Transmission Owner of synchronous condensers (asset owner that is in the best position to ascertain resource capability)

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

² https://www.nerc.com/comm/PC/Power%20Plant%20Modeling%20and%20Verification%20Task%20Force/PPMVTF_White_Paper_MOD-025_Testing.pdf

³ https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_PPMV_for_Synchronous_Machines_-_2018-06-29.pdf

Requested information
Transmission Planner and Planning Coordinator (user of the information provided by the Generator Owner; currently has no responsibility of ensuring accurate data per current MOD-025-2 standard)
Do you know of any consensus building activities⁴ in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The NERC PPMVTF White Paper, approved by NERC RSTC, details the challenges with MOD-025-2. The team deliberated this subject for a significant amount of time, and have identified major issues with the standard that need to be addressed by an SDT. The PPMVTF believes that a significant revision to MOD-025-2 is needed, that testing activities are useful and should be retained, but that the activities can focus on more effective means of collecting useful data for planning models. One dissenting opinion of PPMVTF membership believed the standard should be retired completely and not replaced with an alternative.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
The NERC standards development Project 2020-02 (Transmission-connected Dynamic Reactive Resources) SAR includes MOD-025-2, specifically addressing the applicability of transmission connected reactive devices in addition to generators and synchronous condensers. The SAR on PRC-019-2 submitted to NERC by the System Protection and Control Subcommittee is also related in that there is significant overlap of activities in PRC-019-2 and the development of planning models of machine capability.
This SAR could be combined with those portions of those SARs to address this problem effectively.
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
There are two key industry reference documents on this subject: 1. NERC <i>Reliability Guideline: Power Plant Model Verification and Testing for Synchronous Machines</i>⁵ (July 2018) that provides recommended practices for synchronous machine capability testing. An appendix is devoted to MOD-025-2 testing, and highlights the challenges and inherent errors in MOD-025-2 to obtain useful data that can be applied for planning models. 2. NATF <i>Modeling Reference Document Reporting and Verification of Generating Unit Reactive Power Capability for Synchronous Machines</i>⁶ (April 2015) that describes testing activities per MOD-025-2 and means of ensuring data is sufficient for planning studies.

⁴ Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

⁵ https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_PPMV_for_Synchronous_Machines_-_2018-06-29.pdf

⁶ <https://www.natf.net/docs/natf/documents/resources/planning-and-modeling/natf-reference-document-reporting-and-verification-of-generating-unit-reactive-power-capability-for-synchronous-machines.pdf>

Requested information

Neither industry reference document addresses the identified shortcomings of the standard described above and in NERC PPMVTF *White Paper: Implementation of NERC Standard MOD-025-2*.⁷ These reference materials help industry understand how to implement the standards using best practices, but do not address the reliability gaps created by the standard requirements themselves which is leading to inaccurate data being used in planning assessments.

Reliability Principles

Does this proposed standard development project support at least one of the following Reliability Principles ([Reliability Interface Principles](#))? Please check all those that apply.

☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles

Does the proposed standard development project comply with all of the following [Market Interface Principles](#)?

	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes

⁷ https://www.nerc.com/comm/PC/Power%20Plant%20Modeling%20and%20Verification%20Task%20Force/PPMVTF_White_Paper_MOD-025_Testing.pdf

Market Interface Principles

4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances

Region(s)/ Interconnection	Explanation
N/A	None identified.

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).

☐ Draft SAR reviewed by NERC Staff	☐ Final SAR endorsed by the SC
☐ Draft SAR presented to SC for acceptance	☐ SAR assigned a Standards Project by NERC
☐ DRAFT SAR approved for posting by the SC	☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to PRC-019 to address dispersed power producing resources		
Date Submitted:	4/7/2020		
SAR Requester			
Name:	Chair Jeffrey Iler & Vice Chair Bill Crossland on behalf of the		
Organization:	NERC System Protection and Control Subcommittee (SPCS)		
Telephone:	Chair: (614) 933-2373 Vice Chair: (216) 503-0613	Email:	Chair: jwiler@aep.com Vice Chair: bill.crossland@rfirst.org
SAR Type (Check as many as apply)			
☒ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)		
☒ Revision to Existing Standard	☐ Variance development or revision		
☒ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)		
☐ Withdraw/retire an Existing Standard			
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation	☒ NERC Standing Committee Identified		
☒ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated		
☐ Reliability Standard Development Plan	☒ Industry Stakeholder Identified		
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Reliability Standard PRC-019-2 addresses the reliability issue of miscoordination between generator capability, control systems, and protection functions. However, this standard was developed with a bias toward synchronous generation and does not sufficiently outline the requirements for all generation resource types. The purpose statement of the standard requires modification to be inclusive of all generation resource types. While this class of resources are currently included in the applicability of PRC-019-2, additional clarity is needed in specifying the aspects of dispersed power producing resources that should be coordinated. There are also issues within PRC-019-2 regarding synchronous generation that need to be corrected or clarified to remove ambiguity. These comprehensive updates align with the intent and spirit of the standard.			

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?): This project will enhance reliability by maximizing a generators capability and its ability to support grid stability during system disturbances by requiring the coordination of control systems with equipment capabilities and protection functions of all generation resource types.
Project Scope (Define the parameters of the proposed project): The SDT should develop language that is relevant to all generation resource types. This will include modifications to the purpose statement, the applicability and requirements. Additionally, the SDT should consider modifying Inclusion I4 of the Bulk Electric System (BES) definition and the associated diagrams in the BES Reference Document.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition): 1. Applicable Facilities – Clarification of applicable facilities. a. Clarify Section 4.2.3.1 to state that it pertains to both the individual resources and the plant level voltage controls. [This section indicates that the individual generating units identified through Inclusion I4 of the Bulk Electric System (BES) definition are included only if voltage control for the facility is performed solely at the individual generator; thus, it is ambiguous as to whether this excludes the individual resources from the standard when the plant/facility level or park controller is being used for voltage control.]² b. Verify that static or dynamic reactive compensating devices (i.e., capacitor banks, static VAR compensators, STATCOMs, etc.) and synchronous condensers within BES generating facilities should be subject to the standard since they must be coordinated for protection and plant capability. [The language in footnote 1³ for Requirement R1 implies that reactive compensating devices are not applicable since they are not installed or activated on a generator. These devices are system level voltage regulators and have no effect on an individual inverter capability or limiter functions within an inverter control system; however, they are important to system VAR support and reliability. For example, Type 1 and Type 2 wind turbine generators (WTG) typically employ reactive compensating devices on the collector side of the generator step-up (GSU) transformer. In this case, reactive compensating devices are integral to supporting the systems reactive needs and enhances the reliability of the BES. These devices are not captured by the BES definition because they typically connect at voltages less than 100 kV; however, they should be applicable to the standard for asynchronous and non-rotating resources.]

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

² Reference Section 4.10.10 of the [White Paper](#) from Project 2014-01 Standards Applicability for Dispersed Generation Resources

³ "Limiters or protection functions that are installed and activated on the generator or synchronous condenser."

Requested information

- c. Revise Inclusion I4 of the BES definition and Figures I4-1, I4-2, I4-3, and I4-4 in the BES Reference Document to accurately depict all generation resources.
- 2. **Requirement(s)** – Ensure the language is clear and inclusive of all generation resource types with respect to coordinating control systems, protection functions, and equipment capabilities.
 - d. **Controllers specific to dispersed power producing resources** – The standard is currently biased toward automatic voltage regulating (AVR) control systems used in conjunction with synchronous generation. The standard should address other control systems associated with dispersed power producing resources that are essential to reliability. Typically, inverters have a control system and the facility has a plant controller with a separate control system. The inverter has a control system that may operate in VAR control, Power Factor control, reactive power priority, or active power priority. The plant controller has a control system that may operate in Power Factor or Voltage Control modes. Coordination between any plant/park controller with individual resource control systems must be achieved to prevent unnecessary reduction of the resource.
 - e. **Momentary cessation** – “Momentary cessation” is a function within an Inverter-Based Resource (IBR) control system that reduces active and reactive current to zero when voltage is outside of a defined band.⁴ A reduction in active and/or reactive current can negatively impact reliability, especially during system perturbations, since the function prohibits the IBR from providing support to the BPS during these events.⁵ Ensuring clear language in this standard will ensure that BES generators are not unnecessarily ceasing current injection during abnormal conditions, that any cessation of current is coordinated with equipment capability, and that these functions do not pose a risk to BPS reliability.⁶ Revisions to the standard should consider methods or parameters to eliminate momentary cessation where possible, otherwise ensure it is coordinated with equipment capabilities of the inverter where it cannot be eliminated (for legacy equipment).
 - f. **Controller upgrades and/or changes (e.g., firmware)** – Specify that firmware upgrades are considered “system, equipment or setting changes” under Requirement R2 since these may impact dispersed power producing resource voltage control(s), protection, and limiters.
 - g. **Steady State Stability Limit (SSSL)** – Determine whether the “stability limits” language in Requirement R1.1.2 should be removed from the standard. [Manual SSSL theory is only applicable when a generator AVR is in manual operation mode; however, the standard specifically instructs an entity to assume the AVR is in automatic mode. This assumption is identified because it is industry standard to coordinate the underexcitation limiter with the SSSL since that is the most conservative approach for AVR operation. However, the

⁴ The voltage settings that cause momentary cessation are considered voltage protection settings within the inverter. Other functions within the inverter can cause momentary cessation to operate in a manner similar to a protective function. However, the focus for PRC-019 is on voltage-related functions.

⁵ Including dynamic active power-frequency control and reactive power-voltage control.

⁶ Momentary cessation has been observed in BPS solar PV facilities in all disturbances analyzed by NERC, including but not limited to the Blue Cut Fire, Canyon 2 Fire, Palmdale Roost, and Angeles Forest disturbances.

Requested information	
	protection settings typically coordinate with the machine capabilities and not the manual SSSL.] h. Synchronous condensers – If item ‘d’ remains in the standard, determine whether SSSL should be considered for synchronous condensers. [A synchronous condenser operates in a manner similar to a synchronous generator in terms of voltage regulation and the associated excitation control system. The electrical quantities for a synchronous condenser match the quantities specified in the manual SSSL methodology; however, the machine does not have a prime mover and cannot output real power. This drastically reduces the machines operating region since the unit will only be able to absorb or generate reactive power.] i. Stability limits for other types of generation resources – If item ‘d’ remains in the standard, verify whether a SSSL must be considered for asynchronous and non-rotating generation resources. [Current references to stability limits are all relevant to synchronous machines (AVR in manual mode, fixed excitation voltage, etc.). If consideration of stability is necessary, provide a methodology or implementation guidance for the industry to use (e.g. small signal stability, etc.)]. j. Voltage drop across dispersed power producing resource collector system – Determine whether the voltage drop across the collector system, bus, generator step-up (GSU) transformer, or other facilities should be considered for coordination. k. Time frame to perform coordination – Revise the language in Requirement R2 to remove ambiguity surrounding the timeframe for performing coordination. [The current language can be interpreted as allowing the coordination to be performed 90 days after the “implementation of systems, equipment, or setting changes.” This would allow an entity to put a unit back into service without performing coordination; thus, jeopardizing reliability. The original SDT has confirmed that the 90-day time frame was for scenarios in which an entity discovered a miscoordination.]
	Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
	Costs may include updating firmware on dispersed power producing resources, individual IBRs, park/plant controllers, and other associated equipment, and will vary depending on the approach taken to address the reliability-related risks stated above.
	Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):
	Synchronous generation and dispersed power producing resources may be impacted by the revisions.
	To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
	The team should be made up predominantly by protection engineers with a background in generation protection (synchronous/dispersed power producing resources); preferably industry experts in this field. Additionally, IBR manufacturers and Engineering, Procurement and Construction firms familiar with

Requested information
dispersed power producing resources should be included because of their inherent knowledge of the capabilities and limitations of dispersed power producing resources. Team members should have extensive understanding of generation protection concepts/schemes. In addition, they should have some knowledge of control systems (AVR, IBR's, etc.)
Do you know of any consensus building activities ⁷ in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
No
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
No
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
The NERC SPCS initially attempted to develop Implementation Guidance (IG); however, while developing the IG, the group determined that the standard required additional clarity for IBRs.

Reliability Principles
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.
☒ 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒ 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒ 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐ 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐ 5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐ 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐ 7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐ 8. Bulk power systems shall be protected from malicious physical or cyber attacks.

⁷ Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
<i>None</i>	None

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
1	Project 2007-24	Request for Interpretation - TPL-002 and TPL-003 - Ameren in	Initial Ballot	4/25/2008	5/7/2008	Quorum: 82.61% Approval: 80.73%			
2	Project 2007-26	Request for Interpretation - TPL-002 and TPL-003 - MISO in	Initial Ballot	4/25/2008	5/7/2008	Quorum: 83.01% Approval: 79.89%			
3	Project 2008-04	FAC-010 FAC-011 FAC-014 Order 705 in	Initial Ballot	6/2/2008	6/11/2008	Quorum: 88.83% Approval: 95.43%			
4	Project 2008-07	Interpretation Request - EOP-002 - Brookfield in	Initial Ballot	6/2/2008	6/11/2008	Quorum: 89.67% Approval: 76.47%			
5	Project 2008-04	FAC-010 FAC-011 FAC-014 Order 705 rc	Recirculation Ballot	6/13/2008	6/22/2008	Quorum: 89.36% Approval: 95.21%			
6	Project 2008-09	Request for Interpretation - EOP-001-0 - RECM in	Initial Ballot	6/19/2008	7/2/2008	Quorum: 84.82% Approval: 85.79%			
7	Project 2007-24	Request for Interpretation - TPL-002 and TPL-003 - Ameren rc	Recirculation Ballot	6/27/2008	7/7/2008	Quorum: 83.57% Approval: 79.13%			
8	Project 2007-26	Request for Interpretation - TPL-002 and TPL-003 - MISO rc	Recirculation Ballot	6/27/2008	7/7/2008	Quorum: 83.98% Approval: 78.31%			
9	Pre-2006	IROL Standard - IRO-010 in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.71% Approval: 88.40%			
10	Pre-2006	IROL Standard - IRO-009 in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.63% Approval: 89.44%			
11	Pre-2006	IROL Standard - IRO-008 in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.67% Approval: 91.71%			
12	Project 2006-07	ATC et al Standard - MOD-030 in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.37% Approval: 56.56%			
13	Project 2006-07	ATC et al Standard - MOD-029 in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.67% Approval: 92.62%			
14	Project 2006-07	ATC et al Standard - MOD-028 in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.64% Approval: 79.47%			
15	Project 2006-07	ATC et al Standard - MOD-008 in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.27% Approval: 80.44%			
16	Project 2006-07	ATC et al Standard - MOD-001 in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.02% Approval: 75.97%			
17	Project 2008-10	Request for Interpretation - CIP-006-1 - Progress Energy in	Initial Ballot	8/7/2008	8/16/2008	Quorum: 88.18% Approval: 21.52%			
18	Pre-2006	IROL Standard - IRO-008 rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.72% Approval: 89.49%			
19	Pre-2006	IROL Standard - IRO-009 rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.68% Approval: 86.53%			
20	Pre-2006	IROL Standard - IRO-010 rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.75% Approval: 85.95%			
21	Project 2006-07	ATC et al Standards - MOD-001 rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 94.87% Approval: 76.83%			
22	Project 2006-07	ATC et al Standard - MOD-008 rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.15% Approval: 81.49%			
23	Project 2006-07	ATC et al Standard - MOD-028 rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.54% Approval: 79.34%			
24	Project 2006-07	ATC et al Standard - MOD-029 rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.56% Approval: 92.24%			
25	Project 2006-07	ATC et al Standard - MOD-030 rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.24% Approval: 74.26%			
26	Project 2008-11	Request for Interpretation - VAR-002-1 - ICF Consulting in	Initial Ballot	9/9/2008	9/17/2008	Quorum: 85.78% Approval: 90.37%			
27	Project 2006-07	ATC et al Standard - MOD-004 in	Initial Ballot	9/11/2008	9/21/2008	Quorum: 79.26% Approval: 66.29%			
28	Project 2007-14	Permanent Changes to CI Timing Tables in	Initial Ballot	9/12/2008	9/22/2008	Quorum: 79.74% Approval: 100.00%			
29	Project 2008-07	Request for Interpretation - Brookfield Power - EOP-002 rb	Re-ballot	10/6/2008	10/24/2008	Quorum: 82.61% Approval: 74.67%			
30	Project 2008-13	Request for Interpretation - TOP-002-2 - Orlando Utilities Commission in	Initial Ballot	10/21/2008	10/30/2008	Quorum: 83.33% Approval: 96.94%			
31	Project 2006-01	Project 2006-01 - PER-005-1 in	Initial Ballot	10/27/2008	11/5/2008	Quorum: 90.13% Approval: 82.47%			
32	Project 2006-09	Project 2006-09 - FAC-008-2 - Facility Ratings in	Initial Ballot	10/27/2008	11/5/2008	Quorum: 89.13% Approval: 70.01%			
33	Project 2006-07	ATC et al Standard - MOD-004 rc	Recirculation Ballot	10/28/2008	11/6/2008	Quorum: 91.49% Approval: 83.71%			
34	Project 2006-07	Project 2006-07 (ATC) MOD-030-2 in	Initial Ballot	12/1/2008	12/10/2008	Quorum: 83.77% Approval: 86.51%			
35	Project 2006-09	Project 2006-09 - FAC-008-2 - Facility Ratings rc	Recirculation Ballot	12/10/2008	12/19/2008	Quorum: 93.04% Approval: 57.37%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
36	Project 2008-13	Request for Interpretation - TOP-002-2 - Orlando Utilities Commission rc	Recirculation Ballot	12/10/2008	12/19/2008	Quorum: 87.62% Approval: 97.47%			
37	Project 2006-01	Project 2006-01 - PER-005-1 rc	Recirculation Ballot	12/12/2008	12/22/2008	Quorum: 91.48% Approval: 80.63%			
38	Project 2008-15	Request for Interpretation - CIP-006-1a - US Army COE in	Initial Ballot	1/5/2009	1/14/2009	Quorum: 91.15% Approval: 97.39%			
39	Project 2008-16	TOP-004-2 VSL Revisions in	Initial Ballot	1/5/2009	1/14/2009	Quorum: 91.20% Approval: 93.93%			
40	Project 2008-11	Request for Interpretation - VAR-002-1 - ICF Consulting rc	Recirculation Ballot	1/6/2009	1/15/2009	Quorum: 91.47% Approval: 91.21%			
41	Project 2006-07	Project 2006-07 (ATC) MOD-030-2 rc	Recirculation Ballot	1/20/2009	1/29/2009	Quorum: 85.86% Approval: 86.39%			
42	Project 2008-16	TOP-004-2 VSL Revisions rc	Recirculation Ballot	1/28/2009	2/6/2009	Quorum: 92.59% Approval: 96.06%			
43	Project 2008-15	Request for Interpretation - CIP-006-1a - US Army COE rc	Recirculation Ballot	2/6/2009	2/16/2009	Quorum: 93.81% Approval: 99.12%			
44	Project 2008-09	Interpretation Request - EOP-001 - R1 - RECM in	Initial Ballot	2/27/2009	3/9/2009	Quorum: 89.67% Approval: 89.03%			
45	Project 2008-18	Project 2008-18 Interpretation-Manitoba Hydro in	Initial Ballot	3/19/2009	3/30/2009	Quorum: 89.78% Approval: 92.62%			
46	Project 2008-06	Project 2008-06: CIP-002-1-CIP-009-1 Revisions in	Initial Ballot	4/1/2009	4/10/2009	Quorum: 91.90% Approval: 84.06%			
47	Project 2009-10	Project 2009-10 Interpretation - CMPWG - PRC-005-1 R1 in	Initial Ballot	4/8/2009	4/17/2009	Quorum: 92.70% Approval: 92.71%			
48	Project 2006-03	Project 2006-03 EOP-001 EOP-005 EOP-006 System Restoration and Blackstart in	Initial Ballot	4/14/2009	4/23/2009	Quorum: 89.81% Approval: 76.63%			
49	Project 2008-06	Project 2008-06: CIP-002-1-CIP-009-1 Revisions rc	Recirculation Ballot	4/17/2009	4/27/2009	Quorum: 94.37% Approval: 88.32%			
50	Project 2008-18	Project 2008-18 Interpretation-Manitoba Hydro rc	Recirculation Ballot	4/17/2009	4/27/2009	Quorum: 95.56% Approval: 92.81%			
51	Project 2009-11	Project 2009-11 Interpretation WECC Reliability Coordination Subcommittee IRO-10-1 in	Initial Ballot	4/22/2009	5/1/2009	Quorum: 88.64% Approval: 84.77%			
52	Project 2006-03	Project 2006-03 EOP-001 EOP-005 EOP-006 System Restoration and Blackstart rc	Recirculation Ballot	5/6/2009	5/18/2009	Quorum: 92.08% Approval: 75.39%			
53	Project 2009-15	Project 2009-15 Interpretation - NYISO - MOD-001-1, MOD-029-1 in	initial Ballot	5/25/2009	6/4/2009	Quorum: 85.13% Approval: 82.10%			
54	Project 2009-11	Project 2009-11 Interpretation WECC Reliability Coordination Subcommittee IRO-10-1 rc	Recirculation Ballot	5/26/2009	6/5/2009	Quorum: 90.45% Approval: 85.76%			
55	Project 2009-14	Project 2009-14 Interpretation - PacifiCorp - TPL-002-0a in	Initial Ballot	6/1/2009	6/11/2009	Quorum: 87.10% Approval: 95.71%			
56	Project 2009-08	Project 2009-08 - Nuclear Plant Interface Coordination for Order 716 in	Initial Ballot	6/12/2009	6/22/2009	Quorum: 81.72% Approval: 94.09%			
57	Project 2008-14	Project 2008-14 VSLs for CIP-002-1 through CIP-009-1 in	Initial Ballot	6/15/2009	6/24/2009	Quorum: 87.23% Approval: 83.94%			
58	Project 2008-14	Project 2008-14 VSLs for CIP-002-1 through CIP-009-1 rc	Recirculation Ballot	7/7/2009	7/16/2009	Quorum: 92.77% Approval: 84.96%			
59	Project 2009-15	Project 2009-15 Interpretation - NYISO - MOD-001-1, MOD-029-1 rc	Recirculation Ballot	7/8/2009	7/17/2009	Quorum: 90.26% Approval: 82.25%			
60	Project 2009-08	Project 2009-08 - Nuclear Plant Interface Coordination for Order 716 rc	Recirculation Ballot	7/10/2009	7/20/2009	Quorum: 87.10% Approval: 96.94%			
61	Project 2009-10	Project 2009-10 Interpretation - CMPWG - PRC-005-1 R1 rc	Recirculation Ballot	7/24/2009	8/6/2009	Quorum: 95.26% Approval: 95.62%			
62	Project 2009-14	Project 2009-14 Interpretation - PacifiCorp - TPL-002-0a rc	Recirculation Ballot	7/24/2009	8/6/2009	Quorum: 91.24% Approval: 98.85%			
63	Project 2007-23	Project 2007-23 TPL Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 85.71% Approval: 90.46%			
64	Project 2007-23	Project 2007-23 TOP Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.40% Approval: 89.14%			
65	Project 2007-23	Project 2007-23 PRC Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.32% Approval: 88.26%			
66	Project 2007-23	Project 2007-23 IRO Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.16% Approval: 90.15%			
67	Project 2007-23	Project 2007-23 INT, PER, and NUC Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 85.71% Approval: 88.63%			
68	Project 2007-23	Project 2007-23 FAC and MOD Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.64% Approval: 87.63%			
69	Project 2007-23	Project 2007-23 CIP, COM, and VAR Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.50% Approval: 85.78%			
70	Project 2007-23	Project 2007-23 BAL Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.28% Approval: 89.56%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
71	Project 2008-08	Project 2008-08 EOP Violation Severity Levels in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 87.98% Approval: 87.31%			
72	Project 2009-17	Project 2009-17 Interpretation - Y-W Electric and Tri-State - PRC-004-1 and PRC-005-1 in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 90.32% Approval: 62.15%			
73	RSDP V7	Reliability Standards Development Procedure - Version 7 - June 2009 rb	Re-ballot	7/27/2009	8/14/2009	Quorum: 84.65% Approval: 74.79%			
74	Project 2009-09	Project 2009-09 - Interpretation - Covanta Energy - CIP-001-1 in	Initial Ballot	8/6/2009	8/17/2009	Quorum: 84.68% Approval: 68.92%			
75	Project 2007-23	Project 2007-23 TPL Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 91.96% Approval: 89.28%			
76	Project 2007-23	Project 2007-23 BAL Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.04% Approval: 89.41%			
77	Project 2007-23	Project 2007-23 CIP, COM, and VAR Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.41% Approval: 84.64%			
78	Project 2007-23	Project 2007-23 FAC and MOD Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.67% Approval: 88.04%			
79	Project 2007-23	Project 2007-23 INT, PER, and NUC Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.17% Approval: 88.73%			
80	Project 2007-23	Project 2007-23 IRO Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 91.96% Approval: 90.77%			
81	Project 2007-23	Project 2007-23 PRC Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.31% Approval: 86.93%			
82	Project 2007-23	Project 2007-23 TOP Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.11% Approval: 88.26%			
83	Project 2008-08	Project 2008-08 EOP Violation Severity Levels rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.70% Approval: 85.80%			
84	Order 706-B	Order 706-B Nuclear Implementation Plan in	Initial Ballot	8/19/2009	8/28/2009	Quorum: 81.96% Approval: 97.37%			
85	Project 2008-07	Request for Interpretation - Brookfield Power - EOP-002 rc	Recirculation Ballot	8/20/2009	8/31/2009	Quorum: 86.96% Approval: 70.85%			
86	Project 2009-12	Project 2009-12 - Interpretation - PacifiCorp - CIP-005-1 in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 84.68% Approval: 80.37%			
87	Project 2009-13	Project 2009-13 - Interpretation - PacifiCorp - CIP-006-1 in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 84.92% Approval: 79.04%			
88	Project 2009-18	Project 2009-18 - Withdraw Three Midwest ISO Waivers in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 85.28% Approval: 99.62%			
89	Order 706-B	Order 706-B Nuclear Implementation Plan rc	Recirculation Ballot	9/1/2009	9/10/2009	Quorum: 87.11% Approval: 97.18%			
90	RSDP V7	Reliability Standards Development Procedure - Version 7 - June 2009 rc	Recirculation Ballot	9/2/2009	9/14/2009	Quorum: 86.31% Approval: 76.09%			
91	Project 2008-06	Project 2008-06 Cyber Security (VRFs and VSLs for Version 2 CIP Standards) in	Initial Ballot	9/10/2009	9/21/2009	Quorum: 87.45% Approval: 94.18%			
92	Project 2009-16	Project 2009-16 - Interpretation - WECC - CIP-007-1 in	Initial Ballot	9/9/2009	9/21/2009	Quorum: 85.31% Approval: 100.00%			
93	Project 2006-04	Project 2006-04 - Back-up Facilities - EOP-008-1 in	Initial Ballot	9/16/2009	9/28/2009	Quorum: 82.69% Approval: 72.86%			
94	Project 2009-09	Project 2009-09 - Interpretation - Covanta Energy - CIP-001-1 rc	Recirculation Ballot	9/29/2009	10/9/2009	Quorum: 89.92% Approval: 68.31%			
95	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-1 Revised R1 for Progress Energy	Initial Ballot	9/30/2009	10/12/2009	Quorum: 79.92% Approval: 74.47%			
96	Project 2009-12	Project 2009-12 - Interpretation - PacifiCorp - CIP-005-1 rc	Recirculation Ballot	10/16/2009	10/26/2009	Quorum: 86.29% Approval: 83.25%			
97	Project 2008-06	Project 2008-06 Cyber Security (VRFs and VSLs for Version 2 CIP Standards) rc	Recirculation Ballot	11/2/2009	11/12/2009	Quorum: 88.70% Approval: 94.24%			
98	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 2 in	Initial Ballot	11/5/2009	11/16/2009	Quorum: 85.97% Approval: 98.07%			
99	Project 2009-21	Project 2009-21 - Cyber Security Ninety-day Response in	Initial Ballot	11/20/2009	11/30/2009	Quorum: 89.58% Approval: 88.07%			
100	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 1) in	Initial Ballot	11/19/2009	12/7/2009	Quorum: 85.83% Approval: 58.91%			
101	Project 2009-20	Project 2009-20 - Interpretation - BAL-003-0 - Energy Mark, Inc. in	Initial Ballot	11/20/2009	12/7/2009	Quorum: 87.11% Approval: 93.40%			
102	Project 2009-21	Project 2009-21 - Cyber Security Ninety-day Response rc	Recirculation Ballot	12/3/2009	12/14/2009	Quorum: 93.33% Approval: 85.55%			
103	Project 2009-23	Project 2009-23 - Interpretation - CIP-004-2 - U.S. Army Corps of Engineers in	Initial Ballot	12/1/2009	12/14/2009	Quorum: 86.13% Approval: 72.11%			
104	Project 2009-13	Project 2009-13 - Interpretation - PacifiCorp - CIP-006-1 rc	Recirculation Ballot	12/11/2009	12/23/2009	Quorum: 90.08% Approval: 78.77%			
105	Project 2009-24	Project 2009-24 - Interpretation - FMPA - EOP-005-1 in	Initial Ballot	1/5/2010	1/15/2010	Quorum: 87.68% Approval: 17.79%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
106	Project 2009-25	Project 2009-25 - Interpretation - BPA - BAL-001-01.a and BAL-002-0 in	Initial Ballot	1/5/2010	1/15/2010	Quorum: 88.00% Approval: 34.28%			
107	Project 2009-26	Project 2009-26 - Interpretation - WECC - CIP-004-1 in	Initial Ballot	1/6/2010	1/19/2010	Quorum: 84.21% Approval: 42.24%			
108	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-2	Initial Ballot	1/12/2010	1/22/2010	Quorum: 89.16% Approval: 75.16%			
109	Project 2009-27	Project 2009-27 - Interpretation - TOP-002-2a for FMPAA in	Initial Ballot	2/10/2010	2/22/2010	Quorum: 84.98% Approval: 90.82%			
110	Project 2009-28	Project 2009-28 - Interpretation - EOP-001-1 and EOP-001-2 for FMPP in	Initial Ballot	2/10/2010	2/22/2010	Quorum: 87.36% Approval: 91.79%			
111	Project 2009-29	Project 2009-29 - Interpretation - TOP-002-2a for FMPP in	Initial Ballot	2/11/2010	2/22/2010	Quorum: 84.34% Approval: 84.56%			
112	Project 2009-19	Project 2009-19 - Interpretation - BAL-002-0 Northwest Power Pool RSG in	Initial Ballot	2/15/2010	2/26/2010	Quorum: 89.83% Approval: 48.60%			
113	Project 2009-20	Project 2009-20 - Interpretation - BAL-003-0 - Energy Mark, Inc. rc	Recirculation Ballot	2/16/2010	2/26/2010	Quorum: 92.44% Approval: 91.90%			
114	Project 2009-30	Project 2009-30 - Interpretation - PRC-001-1 for WPSC in	Initial Ballot	2/15/2010	2/26/2010	Quorum: 89.51% Approval: 48.74%			
115	Project 2006-02	Project 2006-02 - Assess Transmission Future Needs - TPL-001-1 in	Initial Ballot	2/19/2010	3/1/2010	Quorum: 91.38% Approval: 35.36%			
116	Project 2009-31	Project 2009-31 - Interpretation - TOP-001-1 for FMPP in	Initial Ballot	3/3/2010	3/16/2010	Quorum: 88.24% Approval: 98.27%			
117	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-2	Recirculation Ballot	3/8/2010	3/18/2010	Quorum: 93.71% Approval: 78.15%			
118	Project 2009-32	Project 2009-32 - Interpretation - EOP-003-1 for FMPP rb	Re-ballot	3/10/2010	3/31/2010	Quorum: 91.37% Approval: 77.66%			
119	Project 2009-23	Project 2009-23 - Interpretation - CIP-004-2 - U.S. Army Corps of Engineers (Revision 1) in	Initial Ballot	3/29/2010	4/8/2010	Quorum: 88.52% Approval: 63.43%			
120	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 3 in	Initial Ballot	4/15/2010	4/26/2010	Quorum: 81.97% Approval: 98.64%			
121	SPM	Standards Process Manual Revisions in	Initial Ballot	4/19/2010	4/29/2010	Quorum: 87.82% Approval: 80.48%			
122	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 2) in	Initial Ballot	4/28/2010	5/10/2010	Quorum: 83.15% Approval: 74.55%			
123	SPM	Standards Process Manual Revisions rc	Recirculation Ballot	4/30/2010	5/10/2010	Quorum: 93.73% Approval: 86.69%			
124	Project 2010-11	Project 2010-11 SAR for TPL Table 1 Order in	Initial Ballot	5/17/2010	5/27/2010	Quorum: 84.41% Approval: 63.75%			
125	Project 2010-09	Project 2010-09: NUC Implementation Plans for CIP Version 2 and Version 3 in	Initial Ballot	5/19/2010	6/1/2010	Quorum: 84.83% Approval: 90.83%			
126	Project 2010-09	Project 2010-09: NUC Implementation Plans for CIP Version 2 and Version 3 rc	Recirculation Ballot	6/22/2010	7/2/2010	Quorum: 89.10% Approval: 87.24%			
127	Project 2006-04	Project 2006-04 - Backup Facilities - Revision 1 in	Initial Ballot	6/23/2010	7/6/2010	Quorum: 89.05% Approval: 79.45%			
128	Project 2006-08	Project 2006-08 - Reliability Coordination - Transmission Loading Relief in	Initial Ballot	6/23/2010	7/6/2010	Quorum: 87.04% Approval: 84.98%			
129	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Initial Ballot	7/7/2010	7/17/2010	Quorum: 86.94% Approval: 43.13%			
130	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Initial Ballot	7/8/2010	7/17/2010	Quorum: 91.12 % Approval: 22.91%			
131	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Non-binding Poll	7/8/2010	7/17/2010	Quorum: 86.00% Approval: 28.00%			
132	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: Protection System definition	Initial Ballot	7/8/2010	7/17/2010	Quorum: 87.85% Approval: 39.35%			
133	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Initial Ballot	7/9/2010	7/19/2010	Quorum: 86.18% Approval: 65.93%			
134	Project 2006-04	Proect 2006-04 - Backup Facilities - Revision 1 rc	Recirculation Ballot	7/16/2010	7/26/2010	Quorum: 93.43% Approval: 85.22%			
135	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Successive Ballot	7/23/2010	8/2/2010	Quorum: 94.70% Approval: 58.61%			
136	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Successive Ballot	7/24/2010	8/3/2010	Quorum: 92.99% Approval: 49.61%			
137	Project 2006-08	Project 2006-08 - Reliability Coordination - Transmission Loading Relief rc	Recirculation Ballot	8/20/2010	8/30/2010	Quorum: 88.26% Approval: 93.93%			
138	Project 2007-04	Project 2007-04 - Certifying System Operators: PER-003-1	Initial Ballot	9/14/2010	9/24/2010	Quorum: 92.73% Approval: 79.17%			
139	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3	Initial Ballot	9/17/2010	9/27/2010	Quorum: 96.46% Approval: 21.77%			
140	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Successive Ballot	9/24/2010	10/4/2010	Quorum: 85.71% Approval: 81.72%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
141	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Successive Ballot	10/2/2010	10/14/2010	Quorum: 84.11% Approval: 84.52%			
142	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 3 rc	Recirculation Ballot	10/4/2010	10/14/2010	Quorum: 88.11% Approval: 99.14%			
143	Project 2009-28	Project 2009-28 - Interpretation - EOP-001-1 and EOP-001-2 for FMPP rc	Recirculation Ballot	10/5/2010	10/15/2010	Quorum: 92.19% Approval: 94.78%			
144	Project 2009-27	Project 2009-27 - Interpretation - TOP-002-2a for FMPAA rc	Recirculation Ballot	10/6/2010	10/16/2010	Quorum: 91.21% Approval: 93.44%			
145	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Recirculation Ballot	10/18/2010	10/28/2010	Quorum: 89.84% Approval: 84.67%			
146	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards) in	Initial Ballot	10/20/2010	11/3/2010	Quorum: 93.66% Approval: 43.33%			
147	Project 2010-10	Project 2010-10 FAC-013-2 Planning Transfer Capability in	Initial Ballot	10/20/2010	11/3/2010	Quorum: 88.54% Approval: 39.85%			
148	2010 SPM	2010 Standard Processes Manual (Proposed Changes) in	Initial Ballot	10/28/2010	11/7/2010	Quorum: 81.61% Approval: 93.72%			
149	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Recirculation Ballot	11/1/2010	11/11/2010	Quorum: 89.41% Approval: 86.83%			
150	2010 SPM	2010 Standard Processes Manual (Proposed Changes) rc	Recirculation Ballot	11/9/2010	11/13/2010	Quorum: 87.00% Approval: 92.88%			
151	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 2) rc	Recirculation Ballot	11/19/2010	12/3/2010	Quorum: 87.81% Approval: 82.41%			
152	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards) sb in	Initial Ballot	12/1/2010	12/10/2010	Quorum: 87.07% Approval: 77.06%			
153	Project 2010-15	Project 2010-15 - Expedited Action Revisions to CIP-005-3	Initial Ballot	12/2/2010	12/11/2010	Quorum: 84.46% Approval: 42.89%			
154	Project 2007-04	Project 2007-04 - Certifying System Operators: PER-003-1	Recirculation Ballot	12/2/2010	12/13/2010	Quorum: 95.50% Approval: 86.91%			
155	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Initial Ballot	12/7/2010	12/16/2010	Quorum: 88.00% Approval: 51.51%			
156	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Successive Ballot	12/10/2010	12/20/2010	Quorum: 79.88% Approval: 44.65%			
157	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Non-binding Poll	12/10/2010	12/20/2010	Quorum: 78.00% Approval: 53.00%			
158	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards) sb rc	Recirculation Ballot	12/20/2010	12/30/2010	Quorum: 90.49% Approval: 80.56%			
159	Project 2010-11	Project 2010-11 TPL Table 1 Footnote B SAR in	Recirculation Ballot	12/27/2010	1/5/2011	Quorum: 90.42% Approval: 83.33%			
160	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.62% Approval: 22.09%	Oppose 12/16/11		
161	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.62% Approval: 33.49%	Oppose 12/16/11		
162	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.60% Approval: 26.82%	Oppose 12/16/11		
163	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.60% Approval: 28.04%	Oppose 12/16/11		
164	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 29.60%	Oppose 12/16/11		
165	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 24.15%	Oppose 12/16/11		
166	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 94.02% Approval: 34.30%	Oppose 12/16/11		
167	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 27.28%	Oppose 12/16/11		
168	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 26.61%	Oppose 12/16/11		
169	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 29.88%	Oppose 12/16/11		
170	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Initial Ballot	12/16/2011	1/6/2011	Quorum: 92.15% Approval: 42.06%	Oppose 12/16/11		
171	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Initial Ballot	12/16/2011	1/6/2011	Quorum: 92.56% Approval: 25.34%	Oppose 12/16/11		
172	Project 2010-10	Project 2010-10: FAC Order 729 in	Initial Ballot	12/30/2010	1/8/2011	Quorum: 83.23% Approval: 58.16%			
173	Project 2010-10	Project 2010-10: FAC Order 729 rc	Recirculation Ballot	1/14/2011	1/23/2011	Quorum: 86.65% Approval: 68.98%			
174	Project 2010-11	Project 2010-11 TPL Table 1 Footnote B SAR rc	Recirculation Ballot	1/26/2011	2/5/2011	Quorum: 93.29% Approval: 86.79%	Support 1/5/11		
175	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Successive Ballot	1/24/2011	2/14/2011	Quorum: 83.95% Approval: 65.71%	Support 2/11/11		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
176	Project 2007-23	Project 2007-23 - Violation Severity Levels	Non-binding Poll	2/9/2011	2/22/2011	Quorum: 78.00% Approval: 72.00%	Support 10/28/10		
177	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Successive Ballot	2/18/2011	2/28/2011	Quorum: 79.28% Approval: 79.34%	Support 2/22/11		
178	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Recirculation Ballot	2/24/2011	3/6/2011	Quorum: 87.35% Approval: 68.83%	Support 2/11/11		
179	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	Initial Ballot	2/25/2011	3/7/2011	Quorum: 87.10% Approval: 49.54%	Support 3/2/11		
180	Project 2010-15	Project 2010-15 - Expedited Action Revisions to CIP-005-4	Successive Ballot	4/19/2011	4/28/2011	Quorum: 79.66% Approval: 38.00%	Oppose 4/19/11		
181	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Initial Ballot	4/21/2011	5/2/2011	Quorum: 86.01% Approval: 48.74%	Abstain 4/26/11		
182	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Non-binding Poll	4/21/2011	5/2/2011	Quorum: 75.58% Approval: 73.00%			
183	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Successive Ballot	5/3/2011	5/12/2011	Quorum: 78.33% Approval: 67.00%	No Recommendation		
184	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Non-binding Poll	5/3/2011	5/12/2011	Quorum: 75.00% Approval: 66.00%			
185	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Recirculation Ballot	5/12/2011	5/23/2011	Quorum: 91.25% Approval: 78.92%	Support 5/12/11		
186	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs - TPL-001 through TPL-006	Successive Ballot	5/18/2011	5/31/2011	Quorum: 92.07% Approval: 73.99%			
187	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs - TPL-001 through TPL-006	Non-binding Poll	5/18/2011	5/31/2011	Quorum: 86.79% Approval: 71.9%			
188	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2, TOP-002-2 and TOP-003-2	Initial Ballot	5/31/2011	6/9/2011	Quorum: 88.47% Approval: 48.64%	Oppose 5/31/11		
189	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2, TOP-002-2 and TOP-003-2	Non-binding Poll	5/31/2011	6/9/2011	Quorum: 84.18% Approval: 41.00%			
190	Project 2007-17	Project 2007-17 – Protection System Maintenance and Testing – PRC-005	Recirculation Ballot	6/20/2011	6/30/2011	Quorum: 82.97% Approval: 64.76%	Support 6/28/11		
191	Project 2007-17	Project 2007-17 – Protection System Maintenance and Testing – PRC-005	Non-binding Poll	6/20/2011	6/30/2011	Quorum: 52.63% Approval: 60.00%			
192	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs	Recirculation Ballot	7/13/2011	7/22/2011	Quorum: 94.33% Approval: 75.37%			
193	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-002-3	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 76.99%	Support 7/22/11		
194	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-005-4	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 75.17%	Support 7/22/11		
195	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-014-2	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 76.27%	Support 7/22/11		
196	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-002-3	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.37% Approval: 93.00%			
197	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-005-4	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.66% Approval: 93.00%			
198	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-014-2	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.37% Approval: 89.00%			
199	Project 2007-09	Project 2007-09 – Generator Verification: MOD-026-1	Initial Ballot	7/22/2011	8/1/2011	Quorum: 90.25% Approval: 46.53%	No Consensus 7/28/11		
200	Project 2007-09	Project 2007-09 – Generator Verification: MOD-026-1	Non-binding Poll	7/22/2011	8/1/2011	Quorum: 88.75% Approval: 56.00%			
201	Project 2007-09	Project 2007-09 – Generator Verification: PRC-024-1	Initial Ballot	7/22/2011	8/1/2011	Quorum: 90.82% Approval: 18.23%	No Consensus 7/28/11		
202	Project 2007-09	Project 2007-09 – Generator Verification: PRC-024-1	Non-binding Poll	7/22/2011	8/1/2011	Quorum: 88.35% Approval: 20.79%			
203	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Initial Ballot	9/19/2011	9/29/2011	Quorum: 84.86% Approval: 61.10%	Support 9/21/11		
204	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Non-binding Poll	9/19/2011	9/29/2011	Quorum: 83.13% Approval: 68.68%			
205	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Definition of BES	Initial Ballot	9/30/2011	10/10/2011	Quorum: 92.97% Approval: 71.68%	No Consensus 10/3/11		
206	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Detailed Information to Support BES Exceptions Request	Initial Ballot	9/30/2011	10/10/2011	Quorum: 89.53% Approval: 64.03%	No Consensus 10/7/11		
207	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Recirculation Ballot	10/4/2011	10/13/2011	Quorum: 87.17% Approval: 86.25%	Support 2/22/11		
208	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Initial Ballot	11/7/2011	11/16/2011	Quorum: 88.05% Approval: 85.53%	Support 11/8/11		
209	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Initial Ballot	11/8/2011	11/17/2011	Quorum: 91.20% Approval: 95.05%	Support 11/8/11		
210	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Initial Ballot	11/9/2011	11/18/2011	Quorum: 88.22% Approval: 86.94%	Support 11/10/11		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
211	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Initial Ballot	11/9/2011	11/18/2011	Quorum: 85.08% Approval: 85.71%	Support 11/10/11		
212	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Initial Ballot	11/9/2011	11/18/2011	Quorum: 84.82% Approval: 85.31%	Support 11/10/11		
213	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-004-2.1	Initial Ballot	11/9/2011	11/18/2011	Quorum: 84.29% Approval: 96.09%	Support 11/10/11		
214	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-x R1 for Progress Energy	Successive Ballot	11/11/2011	11/21/2011	Quorum: 83.53% Approval: 95.99%	Support 11/14/11		
215	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System and Implementation Plan	Recirculation Ballot	11/10/2011	11/21/2011	Quorum: 95.92% Approval: 81.32%	Support 10/3/11		
216	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Detailed Information to Support BES Exceptions Request	Recirculation Ballot	11/10/2011	11/21/2011	Quorum: 93.02% Approval: 81.48%	Support 10/3/11		
217	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Initial Ballot	11/30/2011	12/9/2011	Quorum: 93.92% Approval: 30.82%	Oppose 12/5/11		
218	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Non-binding Poll	11/30/2011	12/9/2011	Quorum: 89.49% Approval: 36.00%			
219	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Initial Ballot	12/2/2011	12/12/2011	Quorum: 87.97% Approval: 36.21%	Oppose 12/5/11		
220	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	12/2/2011	12/12/2011	Quorum: 85.28% Approval: 45.00%			
221	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-x R1 for Progress Energy	Recirculation Ballot	12/9/2011	12/19/2011	Quorum: 88.02% Approval: 96.04%	Support 11/14/11		
222	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Recirculation Ballot	12/12/2011	12/22/2011	Quorum: 90.10% Approval: 92.49%	Support 11/8/11		
223	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 92.00% Approval: 94.58%	Support 11/8/11		
224	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 88.48% Approval: 90.10%	Support 11/10/11		
225	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 87.17% Approval: 85.38%	Support 11/10/11		
226	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 86.91% Approval: 85.03%	Support 11/10/11		
227	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-004-2.1a	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 86.65% Approval: 96.43%	Support 11/10/11		
228	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 59.93%	Oppose 1/9/12		
229	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 77.08 %	Support 1/9/12		
230	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 78.95%	Support 1/9/12		
231	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Non-binding Poll	1/4/2012	1/13/2012	Quorum: 78.27% Approval: 93.00%			
232	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Non-binding Poll	1/9/2012	1/18/2012	Quorum: 76.41% Approval: 71.42%			
233	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Non-binding Poll	1/9/2012	1/19/2012	Quorum: 81.50% Approval: 67.61%			
234	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Non-binding Poll	1/9/2012	1/19/2012	Quorum: 81.50% Approval: 70.28%			
235	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Successive Ballot	1/30/2012	2/9/2012	Quorum: 81.82% Approval: 54.64%	Oppose 2/7/12		
236	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Successive Ballot	1/30/2012	2/9/2012	Quorum: 82.11% Approval: 80.62%	Support 2/7/12		
237	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Successive Ballot	1/30/2012	2/9/2012	Quorum: 81.82% Approval: 80.21%	Support 2/7/12		
238	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 80.35% Approval: 71.35%			
239	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 80.06% Approval: 90.86%			
240	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 79.77% Approval: 84.69%			
241	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 by WECC	Successive Ballot	3/14/2012	3/23/2012	Quorum: 88.55% Approval: 79.61%	Support 3/16/12		
242	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Initial Ballot	3/14/2012	3/23/2012	Quorum: 89.63% Approval: 94.71%	Support 3/16/12		
243	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR-002 for Constellation	Initial Ballot	3/14/2012	3/23/2012	Quorum: 86.92% Approval: 63.09%	Support 3/16/12		
244	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Successive Ballot	3/19/2012	3/29/2012	Quorum: 81.45% Approval: 61.21%			
245	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Successive Ballot	3/19/2012	3/29/2012	Quorum: 80.38% Approval: 41.09%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
246	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	3/19/2012	3/29/2012	Quorum: 84.32% Approval: 73.93%	Support 3/19/12		
247	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Non-binding Poll	3/19/2012	3/29/2012	Quorum: 81.93% Approval: 66.12%			
248	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Successive Ballot	3/30/2012	4/9/2012	Quorum: 80.37% Approval: 85.18%	Support 4/5/12		
249	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Successive Ballot	3/30/2012	4/9/2012	Quorum: 80.10% Approval: 85.01%	Support 4/5/12		
250	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.28% Approval: 41.09%	Oppose 4/16/12		
251	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.04% Approval: 36.84%	Oppose 4/16/12		
252	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.04% Approval: 48.70%%	Oppose 4/16/12		
253	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.82% Approval: 43.72%			
254	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.04% Approval: 38.56%			
255	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.53% Approval: 46.38%			
256	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-005-1.1a	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.95% Approval: 92.41%	Support 4/16/12		
257	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.28%% Approval: 75.44%			
258	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.02% Approval: 87.22%			
259	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.28% Approval: 80.11%			
260	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Non-binding Poll	4/11/2012	4/23/2012	Quorum: 77.21% Approval: 69.84%			
261	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Non-binding Poll	4/11/2012	4/23/2012	Quorum: 77.48% Approval: 67.64%			
262	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 by WECC	Recirculation Ballot	4/20/2012	4/30/2012	Quorum: 90.96% Approval: 80.08%	Support 3/16/12		
263	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Recirculation Ballot	4/20/2012	4/30/2012	Quorum: 92.68% Approval: 94.61%	Support 3/16/12		
264	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 81.72% Approval: 87.34%			
265	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 81.94% Approval: 87.32%			
266	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-005-1.1b	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 90.44% Approval: 93.23%			
267	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 76.84%	Abstain 4/19/12		
268	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 88.11%	Support 4/19/12		
269	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 80.79%	Support 4/19/12		
270	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.63% Approval: 37.37%	Abstain 5/17/12		
271	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.45% Approval: 60.55%	Abstain 5/17/12		
272	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.40% Approval: 38.81%	Abstain 5/17/12		
273	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.98% Approval: 55.08%	Abstain 5/17/12		
274	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.22% Approval: 38.50%	Abstain 5/17/12		
275	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.01% Approval: 45.78%	Abstain 5/17/12		
276	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.19% Approval: 67.19%	Abstain 5/17/12		
277	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.01% Approval: 60.19%	Abstain 5/17/12		
278	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.39% Approval: 47.92%	Abstain 5/17/12		
279	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.39% Approval: 58.23%	Abstain 5/17/12		
280	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Successive Ballot	5/11/2012	5/21/2012	Quorum: 85.12% Approval: 66.23%	Abstain 5/17/12		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
281	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Successive Ballot	5/11/2012	5/21/2012	Quorum: 84.09% Approval: 47.88%	Abstain 5/17/12		
282	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Successive Ballot	5/15/2012	5/24/2012	Quorum: 84.43% Approval: 46.18%			
283	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	5/15/2012	5/24/2012	Quorum: 79.95% Approval: 52.67%			
284	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Initial Ballot	6/11/2012	6/20/2012	Quorum: 84.14% Approval: 21.11%	Oppose 6/13/12		
285	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	6/11/2012	6/20/2012	Quorum: 81.01% Approval: 28.30%			
286	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	6/18/2012	6/27/2012	Quorum: 79.46% Approval: 79.00%			
287	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Non-binding Poll	6/18/2012	6/27/2012	Quorum: 75.00% Approval: 70.21%			
288	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR-002 for Constellation	Successive Ballot	6/18/2012	6/27/2012	Quorum: 85.98% Approval: 68.22%	Support 6/26/12		
289	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Initial Ballot	6/26/2012	7/5/2012	Quorum: 84.24% Approval: 23.82%	Oppose 6/27/12		
290	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Non-binding Poll	6/26/2012	7/5/2012	Quorum: 82.26% Approval: 25.19%			
291	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Recirculation Ballot	6/27/2012	7/6/2012	Quorum: 85.34% Approval: 81.71%			
292	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Recirculation Ballot	6/27/2012	7/6/2012	Quorum: 85.04% Approval: 81.72%			
293	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Non-binding Poll	6/27/2012	7/6/2012	Quorum: 84.16% Approval: 79.16%			
294	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Non-binding Poll	6/27/2012	7/6/2012	Quorum: 83.87% Approval: 86.91%			
295	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Successive Ballot	6/27/2012	7/9/2012	Quorum: 75.37% Approval: 72.16%	No Consensus 7/5/12		
296	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Non-binding Poll	6/27/2012	7/11/2012	Quorum: 75.37% Approval: 73.71%			
297	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision of VAR-002 for Constellation	Recirculation Ballot	7/18/2012	7/27/2012	Quorum: 90.97% Approval: 69.81%	Support 6/26/12		
298	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision of VAR-002 for Constellation	Non-binding Poll	7/18/2012	7/27/2012	Quorum: 81.31% Approval: 60.93%			
299	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Initial Ballot	7/20/2012	7/30/2012	Quorum: 80.39% Approval: 79.28%	Oppose 7/20/12		
300	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Non-binding Poll	7/20/2012	7/30/2012	Quorum: 78.26% Approval: 76.07%			
301	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Initial Ballot	7/24/2012	8/2/2012	Quorum: 83.11% Approval: 54.16%	Oppose 7/20/12		
302	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	8/17/2012	8/27/2012	Quorum: 78.11% Approval: 80.31%	Support 6/22/12		
303	Project 2009-19	Project 2009-19 – Interpretation of BAL-002 by NWPP Reserve Sharing Group	Successive Ballot	8/23/2012	9/4/2012	Quorum: 79.21% Approval: 87.78%	Support 2/22/10		
304	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Initial Ballot	8/29/2012	9/7/2012	Quorum: 86.71% Approval: 37.68%	Support 9/5/12		
305	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Non-binding Poll	8/29/2012	9/7/2012	Quorum: 84.17% Approval: 37.36%			
306	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Recirculation Ballot	9/6/2012	9/17/2012	Quorum: 80.35% Approval: 75.01%			
307	Project 2007-02	Project 2007-02 - Operating Personnel Communication Protocols	Successive Ballot	9/11/2012	9/20/2012	Quorum: 77.70% Approval: 50.57%	Support 9/15/12		
308	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	9/11/2012	9/20/2012	Quorum: 84.05% Approval: 54.07%			
309	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Recirculation Ballot	9/12/2012	9/21/2012	Quorum: 85.36% Approval: 87.34%			
310	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Successive Ballot	9/18/2012	9/27/2012	Quorum: 78.54% Approval: 63.40%	No Consensus 9/27/12		
311	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	9/18/2012	9/27/2012	Quorum: 78.93% Approval: 71.04%			
312	Project 2009-19	Project 2009-19 - Interpretation of BAL-002-0 NWPP Reserve Sharing Group	Recirculation Ballot	9/28/2012	10/8/2012	Quorum: 85.11% Approval: 90.34%	Support 2/22/10		
313	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 74.85%	Support 10/4/12		
314	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.37% Approval: 89.50%	Support 10/4/12		
315	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 85.58%	Support 10/4/12		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
316	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 89.46%	Support 10/4/12		
317	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 92.11%	Support 10/4/12		
318	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 87.73%	Support 10/4/12		
319	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 91.74%	Support 10/4/12		
320	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 91.73%	Support 10/4/12		
321	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 84.60%	Support 10/4/12		
322	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 92.90%	Support 10/4/12		
323	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Successive Ballot	10/1/2012	10/10/2012	Quorum: 78.93% Approval: 94.00%	Support 10/4/12		
324	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Successive Ballot	10/1/2012	10/10/2012	Quorum: 79.13% Approval: 91.59%	Support 10/4/12		
325	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Initial Ballot	10/3/2012	10/12/2012	Quorum: 87.50% Approval: 63.25%	Support 10/4/12		
326	VRFs and VSLs	Revisions to Outstanding VRFs and VSLs	Non-binding Poll	10/10/2012	10/23/2012	Quorum: 78.57% Approval: 73.02%			
327	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Recirculation Ballot	10/15/2012	10/24/2012	Quorum: 81.08% Approval: 80.51%	Support 6/22/12		
328	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 75.55% Approval: 76.50%			
329	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 75.00% Approval: 57.24%			
330	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Successive Ballot	10/19/2012	10/31/2012	Quorum: 83.61% Approval: 68.31%			
331	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 82.34% Approval: 71.53%			
332	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 82.07% Approval: 70.64%			
333	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 75.88% Approval: 77.10%			
334	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 75.40% Approval: 52.72%			
335	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 77.94% Approval: 64.24%			
336	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 78.06% Approval: 68.93%			
337	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 78.51% Approval: 63.63%			
338	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 78.59%	Support 10/4/12		
339	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 92.75%	Support 10/4/12		
340	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 89.73%	Support 10/4/12		
341	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 93.73%	Support 10/4/12		
342	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.53%	Support 10/4/12		
343	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 91.79%	Support 10/4/12		
344	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.47%	Support 10/4/12		
345	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 94.60%	Support 10/4/12		
346	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 88.99%	Support 10/4/12		
347	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.67%	Support 10/4/12		
348	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation Plan	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 83.47% Approval: 94.91%	Support 10/4/12		
349	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 83.47% Approval: 93.23%	Support 10/4/12		
350	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Recirculation Ballot	10/24/2012	11/5/2012	Quorum: 85.14% Approval: 71.39%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
351	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	10/24/2012	11/5/2012	Quorum: 78.93% Approval: 71.04%			
352	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Successive Ballot	10/26/2012	11/6/2012	Quorum: 82.04% Approval: 76.08%	Support 11/5/12		
353	Project 2010-11	Project 2010-11 TPL footnote b Initial Ballot October 2012 in	Initial Ballot	11/9/2012	11/19/2012	Quorum: 80.45% Approval: 56.18%			
354	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Initial Ballot	11/26/2012	12/5/2012	Quorum: 84.81% Approval: 72.57%	Oppose 12/5/12		
355	Project 2013-02	Project 2013-02 - Paragraph 81	Initial Ballot	11/30/2012	12/10/2012	Quorum: 75.77% Approval: 96.45%	Support 12/10/12		
356	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Successive Ballot	12/4/2012	12/13/2012	Quorum: 76.78% Approval: 53.57%	No Consensus 12/13/12		
357	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	12/4/2012	12/13/2012	Quorum: 77.22% Approval: 57.91%			
358	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Successive Ballot	12/7/2012	12/17/2012	Quorum: 76.47% Approval: 33.23%	Oppose 12/17/12		
359	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Non-binding Poll	12/7/2012	12/17/2012	Quorum: 75.58% Approval: 34.80%			
360	Project 2012-INT-05	Interpretation 2012-INT-05: CIP-002-3 for OGE	Initial Ballot	12/11/2012	12/20/2012	Quorum: 84.50% Approval: 95.60%	Support 12/19/12		
361	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Successive Ballot	12/11/2012	12/20/2012	Quorum: 83.24% Approval: 84.48%	Support 12/19/12		
362	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.89% Approval: 73.06%			
363	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 79.00% Approval: 79.36%			
364	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.68% Approval: 74.27%			
365	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 85.87% Approval: 73.63%			
366	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.19% Approval: 76.53%			
367	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Successive Ballot	1/2/2013	1/11/2013	Quorum: 78.16% Approval: 60.31%	Support 1/11/13		
368	Project 2007-09	Project 2007-09 - Generator Verification - PRC-024-1	Non-binding Poll	1/2/2013	1/11/2013	Quorum: 76.38% Approval: 55.68%			
369	Project 2010-11	Project 2010-11 Successive Ballot December 2012 in	Successive Ballot	1/2/2013	1/11/2013	Quorum: 85.47% Approval: 65.77%	No Consensus 1/11/13		
370	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-012-1	Initial Ballot	1/4/2013	1/14/2013	Quorum: 83.94% Approval: 21.80%	Oppose 1/11/13		
371	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-012-1	Non-binding Poll	1/4/2013	1/14/2013	Quorum: 82.23% Approval: 24.27%			
372	Project 2013-02	Project 2013-02 - Paragraph 81	Recirculation Ballot	1/8/2013	1/17/2013	Quorum: 84.60% Approval: 95.22%	Support 12/10/12		
373	Project 2012-INT-05	Interpretation 2012-INT-05: CIP-002-3 for OGE	Recirculation Ballot	1/14/2013	1/23/2013	Quorum: 87.13% Approval: 99.09%	Support 12/19/12		
374	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Recirculation Ballot	1/18/2013	1/28/2013	Quorum: 85.90% Approval: 85.57%	Support 12/19/12		
375	Project 2010-11	Project 2010-11 Recirculation Ballot Jan 2013 in	Recirculation Ballot	1/22/2013	1/31/2013	Quorum: 88.55% Approval: 69.63%	No Consensus 1/11/13		
376	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Recirculation Ballot	1/22/2013	1/31/2013	Quorum: 85.67% Approval: 77.61%	Oppose 12/5/12		
377	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Successive Ballot	2/11/2013	2/20/2013	Quorum: 77.62% Approval: 50.66%	Support 9/5/12		
378	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Non-binding Poll	2/11/2013	2/20/2013	Quorum: 75.38% Approval: 50.60%			
379	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Successive Ballot	2/15/2013	2/28/2013	Quorum: 78.80% Approval: 89.01%	Support 1/11/13		
380	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Non-binding Poll	2/15/2013	2/28/2013	Quorum: 76.38% Approval: 84.24%			
381	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Initial Ballot	3/1/2013	3/11/2013	Quorum: 76.36% Approval: 54.65%			
382	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Successive Ballot	3/13/2013	3/22/2013	Quorum: 77.48% Approval: 84.27%	No Consensus 3/22/13		NPCC to abstain - international nature of the ERO and BPS is not used in Reliability Standards
383	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	Initial Ballot	3/13/2013	3/22/2013	Quorum: 88.58% Approval: 97.18%	Support 3/14/13		
384	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	Initial Ballot	3/13/2013	3/22/2013	Quorum: 88.52% Approval: 98.89%	Support 3/14/13		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
385	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Recirculation Ballot	3/18/2013	3/27/2013	Quorum: 81.33% Approval: 89.44%	Support 1/11/13		
386	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Successive Ballot	3/27/2013	4/5/2013	Quorum: 78.39% Approval: 57.50%	No Consensus 4/4/13		The RSC did not reach a full consensus however the majority of respondents had indicated they will support the standard - see comment form for further details. Some believe the standard is not necessary and that existing whitepapers alleviate the need for it. In recognition of the NERC BOT's expectations that COM-003 will be approved by the industry and brought before them for approval, NPCC has voted affirmatively and will supply comments for the record outlining our concerns.
387	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	3/27/2013	4/5/2013	Quorum: 77.97% Approval: 54.28%			
388	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.60% Approval: 66.98%	No Consensus 4/23/13		The majority of NPCC's Balancing Authorities have indicated support for the standard, however NPCC as the Regional Entity has concerns based on results of the field trials that were conducted. These field trials have indicated the potential for an increased number of SOL violations as well as potential for increased ACE due to large inadvertent flows with the proposed BAAL limits based on frequency triggers. To be respectful of the positions of the NPCC BAs who will have to implement this new methodology and the support expressed, NPCC as the Regional Entity will cast an Abstention
389	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-002-2	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.51% Approval: 42.75%	Oppose 4/23/13		There is a lack of technical justification for the 500 MW threshold within the standard- NPCC will submit suggested improvements
390	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-013-1	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.51% Approval: 23.84%	Oppose 4/23/13		Losses of large blocks of load are typically caused by coincident transmission contingencies. Excessive and uninformed adjustments made to generation in order to bring the ACE to zero may well lead to further transmission issues. NPCC will submit suggested improvements

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of “Ballot Periods” column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
391	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
392	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-002-2	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
393	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-013-1	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
394	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Recirculation Ballot	4/18/2013	4/29/2013	Quorum: 80.70% Approval: 88.15%	No Consensus 3/22/13		
395	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Successive ballot	5/15/2013	5/24/2013	Quorum: 81.25% Approval: 69.23%	Support 5/23/13		The Regional Standard Committee has not expressed any concerns of significance that would warrant a ballot to reject, therefore the RSC recommends a yes vote, “Affirmative”, to accept the standard
396	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Non-binding Poll	5/15/2013	5/24/2013	Quorum: 80.17% Approval: 61.11%			
397	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	Successive Ballot	6/24/2013	7/3/2013	Quorum: 77.65% Approval: 52.71%			
398	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	Non-binding Poll	6/24/2013	7/3/2013	Quorum: 77.12% Approval: 52.48%			
399	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Initial Ballot	7/3/2013	7/12/2013	Quorum: 85.53% Approval: 49.73%			
400	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	Successive Ballot	7/10/2013	7/19/2013	Quorum: 76.32% Approval: 58.36%	No Consensus 7/19/13 [Due to the concerns expressed over the potential actions by the NERC BOT and FERC as well as the incremental improvement of the standard over the previous versions, NPCC as the Regional Entity will support the standard and submit comments.]		The majority of RSC member organizations support the standard as written however some members expressed concern that in order to measure compliance with R1 and R2, the standard will require all Reliability Directives to be investigated to determine if RC approved and documented communication protocols have been violated. Also it was identified that TO, BA communication protocols would have to approved by the RC potentially causing some legal issues if protocols aren’t approved and casts question on the enforcement of those protocols. NPCC will be submitting some helpful comments should the standard pass and some non-substantive revision be performed prior to the “final” (previously named recirculation) ballot.
401	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	Non-binding Poll	7/10/2013	7/19/2013	Quorum: 76.20% Approval: 55.37%			
402	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	Successive Ballot	7/10/2013	7/19/2013	Quorum: 85.05% Approval: 72.43%	Support 7/19/13		
403	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	Non-binding Poll	7/10/2013	7/19/2013	Quorum: 82.51% Approval: 64.59%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
404	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Final Ballot	7/16/2013	7/25/2013	Quorum: 92.31% Approval: 74.54%	No Consensus 7/22/13		The RSC has not reached a full consensus however the majority are in support. Issues outstanding for those not in support are concern over "hitting limits" more frequently and potential issues with BA's potentially "dragging" on the interconnection. NPCC will be voting affirmative on the standard.
405	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023-3	Initial Ballot	7/26/2013	8/5/2013	Quorum: 80.05% Approval: 93.00%	Support 8/5/13		
408	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025-1	Final Ballot	8/2/2013	8/12/2013	Quorum: 89.13% Approval: 76.52%	Support 8/12/13		
406	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Initial Ballot	8/2/2013	8/12/2013	Quorum: 76.32% Approval: 62.74%	Support 8/9/13		
407	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Non-binding Poll	8/2/2013	8/12/2013	Quorum: 75.89% Approval: 55.45%			
409	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Initial Ballot	8/14/2013	8/23/2013	Quorum: 78.33% Approval: 79.42%	Support 8/23/13		
410	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Non-binding Poll	8/14/2013	8/23/2013	Quorum: 77.45% Approval: 81.37%			
411	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Ballot	8/16/2013	8/26/2013	Quorum: 76.14% Approval: 51.10%	No Consensus 8/26/13		NPCC to support with comments
412	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Non-binding Poll	8/16/2013	8/26/2013	Quorum: 75.98% Approval: 53.29%			
413	Project 2010-01	Project 2010-01 - Training - PER-005-2	Ballot	8/23/2013	9/3/2013	Quorum: 75.25% Approval: 34.46%	No Consensus 8/31/13		NPCC to support with comments The most contentious issues raised by RSC members was surrounding the Control Center definition and the potential to vastly expand those needing training subject to the standard and compliance and that there was no need for a standard, rather, the FERC Directives should be addressed through other means.
414	Project 2010-01	Project 2010-01 - Training - PER-005-2	Non-binding Poll	8/23/2013	9/3/2013	Quorum: 80.45% Approval: 34.24%			
415	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	Ballot	8/23/2013	9/3/2013	Quorum: 81.89% Approval: 43.79%	Oppose 8/31/13		The standard, in the view of the group, has extensive issues including but not limited to, applicability issues, lacks clarity, missing measures, quality, and other substantive issues. NPCC will be submitting detailed comments to address these issues. The RSC does not believe it would be beneficial to support the standard at this point as the next step, if it fails the initial ballot, would still require an additional ballot prior to moving to recirculation due to the substantive changes that are needed for the next revision. NPCC will be submitting helpful comments to NERC and supporting the drafting team effort.

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
416	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	Non-binding Poll	8/23/2013	9/3/2013	Quorum: 79.95% Approval: 44.23%			
417	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	Ballot	8/26/2013	9/4/2013	Quorum: 82.29% Approval: 41.24%	Support 8/31/13		
418	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	Non-binding Poll	8/26/2013	9/4/2013	Quorum: 79.66% Approval: 40.00%			
419	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Ballot	8/26/2013	9/4/2013	Quorum: 81.96% Approval: 55.76%	Support 8/31/13		
420	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Non-binding Poll	8/26/2013	9/4/2013	Quorum: 80.35% Approval: 58.97%			
421	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Additional Ballot	8/26/2013	9/4/2013	Quorum: 78.68% Approval: 66.11%	Support 8/31/13		
426	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023-3	Final Ballot	9/4/2013	9/13/2013	Quorum: 85.93% Approval: 90.83%	Support 8/5/13		
422	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	Ballot	9/6/2013	9/16/2013	Quorum: 76.15% Approval: 58.23%	No Consensus 9/12/13		
423	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	Non-binding Poll	9/6/2013	9/16/2013	Quorum: 75.69% Approval: 59.66%			
424	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	Final Ballot	9/11/2013	9/20/2013	Quorum: 91.64% Approval: 98.61%	Support 3/14/13		
425	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	Final Ballot	9/11/2013	9/20/2013	Quorum: 90.98% Approval: 98.92%	Support 3/14/13		
427	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Additional Ballot	10/9/2013	10/21/2013	Quorum: 77.58% Approval: 88.75%	Support 10/16/13		
428	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Non-binding Poll	10/9/2013	10/21/2013	Quorum: 75.89% Approval: 90.04%			
429	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Final Ballot	10/16/2013	10/25/2013	Quorum: 85.71% Approval: 85.38%			
430	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Additional Ballot	10/18/2013	10/29/2013	Quorum: 75.83% Approval: 72.55%	Support 10/21/13		
431	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Final Ballot	10/25/2013	11/4/2013	Quorum: 86.90% Approval: 91.95%			
432	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Additional Ballot	10/25/2013	11/7/2013	Quorum: 76.67% Approval: 58.24%	No Consensus 11/1/13		
433	Project 2010-01	Project 2010-01 - Training - PER-005-2	Additional Ballot	11/1/2013	11/12/2013	Quorum: 76.23% Approval: 56.48%	Support 11/11/13		
434	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Initial Ballot	11/4/2013	11/13/2013	Quorum: 76.12% Approval: 67.35%	Support 11/5/13		
435	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-006-4	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 75.58%	Support 11/5/13		
436	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-009-2	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 68.40%	Support 11/5/13		
437	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 58.03%	Support 11/5/13		
438	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-011-1	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.52% Approval: 71.35%	Support 11/5/13		
439	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Initial Ballot	11/4/2013	11/15/2013	Quorum: 76.42% Approval: 77.82%	Support 11/5/13		
440	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Final Ballot	11/8/2013	11/18/2013	Quorum: 81.68% Approval: 74.34%	Support 10/21/13		
441	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Additional Ballot	11/8/2013	11/20/2013	Quorum: 81.69% Approval: 82.97%	No Consensus 8/26/13		
442	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1	Additional Ballot	11/8/2013	11/20/2013	Quorum: 79.05% Approval: 73.46%	Support 8/31/13		
443	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Additional Ballot	11/8/2013	11/20/2013	Quorum: 79.84% Approval: 69.42%	Support 8/31/13		
444	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Additional Ballot	11/13/2013	11/22/2013	Quorum: 80.54% Approval: 57.59%	Support 8/31/13		
445	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4	Additional Ballot	11/15/2013	11/25/2013	Quorum: 80.81% Approval: 69.43%			
446	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-002-3	Additional Ballot	11/15/2013	11/25/2013	Quorum: 81.06% Approval: 66.09%			
447	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2	Additional Ballot	12/2/2013	12/12/2013	Quorum: 75.29% Approval: 64.24%	No Consensus 12/9/13	Affirmative	

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of “Ballot Periods” column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
448	Project 2007-11	Project 2007-11 Disturbance Monitoring - PRC-002-2	Initial Ballot	12/6/2013	12/16/2013	Quorum: 82.25% Approval: 43.29%	No Consensus 12/15/13	Affirmative	Highlights of comments received expressed: • Agreement with the methodology to determine BES locations for which data had to be captured • Use of the term “locations” • DDR for Flowgates, IROLs • Clarification needed for some data that is to be captured • Editorial suggestions
449	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1	Final Ballot	12/6/2013	12/16/2013	Quorum: 87.53% Approval: 77.49%	Support 8/31/13	Affirmative	
450	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-006-4	Final Ballot	12/10/2013	12/20/2013	Quorum: 85.07% Approval: 80.77%	Support 11/5/13	Affirmative	
451	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-009-2	Final Ballot	12/10/2013	12/20/2013	Quorum: 85.07% Approval: 72.86%	Support 11/5/13	Affirmative	
452	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-011-1	Final Ballot	12/10/2013	12/20/2013	Quorum: 84.78% Approval: 72.91%	Support 11/5/13	Affirmative	
453	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Final Ballot	12/11/2013	12/20/2013	Quorum: 87.16% Approval: 86.40%	No Consensus 8/26/13	Affirmative	
454	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4	Final Ballot	12/13/2013	12/23/2013	Quorum: 84.34% Approval: 75.35%		Affirmative	
455	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-027-1	Additional Ballot	12/9/2013	12/31/2013	Quorum: 76.60% Approval: 65.71%	No Consensus 12/27/13	Affirmative	
456	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Additional Ballot	1/10/2014	1/21/2014	Quorum: 76.92% Approval: 81.41%	Support 8/31/13	Affirmative	
457	Project 2010-01	Project 2010-01 - Training - PER-005-2	Additional Ballot	1/8/2014	1/22/2014	Quorum: 79.12% Approval: 74.63%	Support 11/11/13	Affirmative	
458	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Additional Ballot	1/10/2014	1/22/2014	Quorum: 75.22% Approval: 81.19%	Support 11/5/13	Affirmative	
459	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Additional Ballot	1/10/2014	1/22/2014	Quorum: 75.22% Approval: 90.23%	Support 11/5/13	Affirmative	
460	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Additional Ballot	1/16/2014	1/29/2014	Quorum: 76.12% Approval: 92.17%	Support 11/5/13	Affirmative	
461	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Additional Ballot	1/22/2014	1/31/2014	Quorum: 76.03% Approval: 71.86%	No Consensus 11/1/13	Affirmative	Ballot Period Extended to 2/4/14
462	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Final Ballot	1/27/2014	2/5/2014	Quorum: 83.88% Approval: 83.44%	Support 11/5/13	Affirmative	
463	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Final Ballot	1/27/2014	2/5/2014	Quorum: 83.58% Approval: 91.51%	Support 11/5/13	Affirmative	
464	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Final Ballot	1/27/2014	2/5/2014	Quorum: 82.49% Approval: 82.45%	Support 8/31/13	Affirmative	
465	Project 2010-01	Project 2010-01 - Training - PER-005-2	Final Ballot	1/27/2014	2/5/2014	Quorum: 84.02% Approval: 77.06%	Support 11/11/13	Affirmative	
466	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Final Ballot	1/31/2014	2/10/2014	Quorum: 81.79% Approval: 90.12%	Support 11/5/13	Affirmative	
467	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Additional Ballot	2/21/2014	3/3/2014	Quorum: 75.06% Approval: 62.63%	Support 9/5/12	Affirmative	Ballot Period Extended to 3/11/14
468	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Final Ballot	3/28/2014	4/7/2014	Quorum: 78.21% Approval: 77.62%	Support 3/28/14	Affirmative	
469	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Additional Ballot	4/1/2014	4/10/2014	Quorum: 76.92% Approval: 83.40%	Support 8/31/13	Affirmative	
470	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-002-3	Additional Ballot	4/4/2014	4/14/2014	Quorum: 78.03% Approval: 82.40%		--	
471	Project 2014-04	Project 2014-04 Physical Security - CIP-014-1	Initial Ballot	4/20/2014	4/24/2014	Quorum: 88.60% Approval: 82.07%	Support 4/23/14	Abstain	
472	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Final Ballot	4/25/2014	5/5/2014	Quorum: 80.37% Approval: 90.00%	Support--4/25/14	Affirmative	
473	Project 2013-04	Project 2013-04 - Voltage and Reactive Control - VAR-001-4, VAR-002-3	Final Ballot	4/23/2014	5/5/2014	Quorum: 83.84% Approval: 88.26%	Support--4/10/14	Affirmative	
474	Project 2014-04	Project 2014-04 - Physical Security - CIP-014-1	Final Ballot	5/1/2014	5/5/2014	Quorum: 92.53% Approval: 85.61%	Support--4/23/14	Abstain	
475	Project 2010-02	Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2	Initial Ballot	5/6/2014	5/15/2014	Quorum: 85.79%/79.08% Approval: 86.28%/78.81%	No Consensus--5/15/14	Reject	
476	Project 2012-13	Project 2012-13 - NUC - Nuclear Plant Interface Coordination	Initial Ballot	5/13/2014	5/22/2014	Quorum: 80.60% Approval: 97.36%	Support--5/20/14	Affirmative	
477	Project 2007-17.3	Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) - PRC-005-X	Initial Ballot	5/23/2014	6/2/2014	Quorum: 85.42% Approval: 47.89%	Support	Affirmative	

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
478	Project 2010-13.3	Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings	Initial Ballot	5/30/2014	6/9/2014	Quorum: 79.06% Approval: 17.02%	Does not Support--6/6/14	Negative	
475	Project 2010-02	Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2	Final Ballot	6/12/2014	6/23/2014	Quorum: 89.03%/83.46% Approval: 89.03%/83.46%	Support	Affirmative	
479	Project 2007-11	Project 2007-11 - Disturbance Monitoring - PRC-002-2	Additional Ballot	6/13/2014	6/23/2014	Quorum: 77.69% Approval: 52.29%	Support	Affirmative	Extended to achieve a quorum.
480	Project 2010-05.1	Project 2010-05.1 - Protection System: Phase 1 (Misoperations) - PRC-004	Additional Ballot	6/20/2014	7/9/2014	Quorum: 76.98% Approval: 74.53%	Support	Affirmative	Extended to achieve a quorum.
481	Project 2014-03	Project 2014-03 - Revisions to TOP/IRO Reliability Standards	Ballot	6/23/2014	7/2/2014	Quorum: 82.32%/82.59%/82.59 %/82.85%/82.85%/82.06%/82.59%/82.85%/82.85%/81.00%/80.74 % Approval: 68.57%/36.94%/47.87 %/60.26%/61.67%/57.94%/30.99%/62.18%/63.07%/62.64%/64.70 %	No Consensus--6/24/14	Affirmative Negative Affirmative Affirmative Affirmative Negative Affirmative Affirmative	
482	Project 2012-13	Project 2012-13 NUC - Nuclear Plant Interface Coordination	Final Ballot	6/24/2014	7/3/2014	Quorum: 88.63% Approval: 97.23%	Support--6/23/14	Affirmative	
483	Project 2014-02	Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions Rich HTML Content 1 http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx	Final Ballot	7/7/2014	7/16/2014	Quorum: 80.73%/80.49%/80.00 %/80.24%/80.24%/80.49%/80.24%/78.29% Approval: 35.67%/80.76%/76.24 %/78.41%/85.32%/49.42%/82.55%/78.58%	CIP-003 No CIP-004 Yes CIP-006 Yes CIP-007 Yes CIP-009 Yes CIP-010 Yes CIP-011 Yes Definitions Yes Support--7/14/14		
484	Project 2010-05.2	Project 2010-05.2 -- Special Protection Systems (Phase 2 of Protection Systems)	Final Ballot	7/16/2014	7/25/2014	Quorum: 78.92% Approval: 58.88%	Support--7/23/14		
485	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Final Ballot	7/18/2014	7/28/2014	Quorum: 79.49%/80.15%/80.00 %/80.83%/80.36% Approval: 91.38%/92.20%/89.51 %/90.58%/87.09%	Support--7/24/14	Affirmative	
486	Project 2012-13	Project 2013-03 Geomagnetic Disturbance Mitigation	Final Ballot	7/21/2014	7/30/2014	Quorum: 82.67% Approval: 55.77%		Affirmative	
487	Project 2012-13	Project 2008-02 Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS)	Initial Ballot	7/29/2014	8/7/2014	Quorum: 76.37% Approval: 76.91%		Affirmative	
488	Project 2012-13	Project 2009-03 Emergency Operations	Initial Ballot	8/6/2014	8/15/2014	Quorum: 77.66% Approval: 42.27%	Negative--8/14/14	Negative	
489	Project 2014-01	Project 2010-05.1 - Protection System: Phase 1 (Misoperations) - PRC-004	Final Ballot	7/29/2014	8/7/2014	Quorum: 77.94% Approval: 79.75%	Support	Affirmative	
490	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Final Ballot	8/27/2014	9/5/2014	Quorum: 85.32%/86.01% Approval: 95.35%/95.86%	Support	Affirmative	
491	Project 2007-17.3	(Sudden Pressure Relays) - PRC-005-X	Additional Ballot	9/3/2014	9/12/2014	Quorum: 84.33% Approval: 76.03%	Support--9/4/14	Affirmative	
492	Project 2014-03	Project 2014-03 - Revisions to TOP/IRO Reliability Standards	Additional Ballot	9/10/2014	9/19/2014	Quorum: 85.75%/84.96%/84.96 %/85.22%/84.96%/85.22%/85.49%/85.22%/86.28%/83.11%/83.91 %	TOP-001-3: Negative TOP-002-4: Affirmative TOP-003-3: Affirmative IRO-001-4: No consensus however the majority indicated an Affirmative vote IRO-002-4: Negative		

Last RSC Meeting

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
						Approval: 76.12%/74.23%/75.67 %/85.49%/75.96%/78. 67%/48.73%/78.87%/ 87.03%/93.34%/90.13 %	IRO-008-2: No consensus, a majority indicated a Negative and the others indicated abstention IRO-010-2: Affirmative IRO-014-3: Negative IRO-017-1: Affirmative Implementation Plan and Definitions: Affirmative 9/18/14		
493	Project 2010-14.1	Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	Additional Ballot	9/23/2014	10/2/2014	Quorum: 79.94%	Negative--10/1/14		
						Approval: 46.73%			
494	Project 2010-13.3	Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings	Additional Ballot	9/26/2014	10/6/2014	Quorum: 79.01%	Affirmative--10/1/14		
						Approval: 53.02%			
495	Project 2012-13	Project 2008-02 Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS)	Additional Ballot	9/29/2014	10/8/2014	Quorum: 83.24%/84.82% Approval: 81.40%	Affirmative--10/7/14	Affirmative	
						Approval: 80.69%/84.05%			
496	Project 2012-13	Project 2013-03 Geomagnetic Disturbance Mitigation	Additional Ballot	10/1/2014	10/10/2014	Quorum: 82.93% Approval: 57.95%	Affirmative--10/7/14		
497	Project 2010-05.2	Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)	Additional Ballot	10/3/2014	10/14/2014	Quorum: 80.54% Approval: 75.79%	Affirmative--10/7/14		
						Approval:			
498	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Additional Ballot	10/7/2014	10/16/2014	Quorum: 81.91%/82.12% Approval: 94.92%/94.37%	Affirmative--10/14/14		
499	Project 2014-02	Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions	Additional Ballot	10/8/2014	10/17/2014	Quorum: 84.63%/84.15%/84.15 %/83.90%/83.41%/83. 66%/83.96%/84.49%/83. 96%/83.96%/84.22 %/84.49%/84.22% Approval: 93.21%/68.09%/74.25 %/79.91%/85.68%/89. 01%/91.79%/81.34%/96.63%/96.63%/95.52 %/85.93%/98.13%	CIP-003-6 no consensus CIP-010-2 no consensus New Definitions-Affirmative Updated Definitions-Affirmative Implementation Plan-Affirmative Version X Materials-Affirmative Non-binding polls-Affirmative	CIP-003-6 and CIP-010-2 Affirmative	
500	Project 2009-03	Project 2009-03 Emergency Operations	Additional Ballot	10/10/2014	10/20/2014	Quorum: 80.93% Approval: 70.41%	Affirmative--10/17/14		
501	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards (IRO-001-4, IRO-002-4, IRO-010-2, two Definitions, and Implementation Plan)	Final Ballot	10/10/2014	10/20/2014	Quorum: 90/77%/89.97%/89.97 %/88.39%/88.39% Approval: 82.64%/85.96%/86.22 %/94.07%/91.84%	Affirmative--10/17/14		
502	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards (TOP-002-4, TOP-003-3, IRO-008-2, IRO-014-3, and IRO-017-1)	Final Ballot	10/10/2014	10/20/2014	Quorum: 89.71%/88.39%/89.71 %/89.71%/89.97% 84.76%/86.55%/83.73 %/89.88%/82.58%	Affirmative--10/17/14		
503	Project 2007-11	Project 2007-11 Disturbance Monitoring	Additional Ballot	10/10/2014	10/21/2014	Quorum: 77.69% Approval: 71.38%	Affirmative--10/17/14		
504	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Additional Ballot	10/10/2014	10/22/2014	Quorum: 85.13%/83.29% Approval: 94.75%/93.98%	Affirmative--10/20/14		
505	Project 2014-03	Project 2007-17.3 (PRC-005-X) Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays)	Final Ballot	10/20/2014	10/29/2014	Quorum: 88.25%	Affirmative--10/28/14		
						Approval: 74.14%			
506	Project 2014-03	Project 2008-02 Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS)	Final Ballot	10/28/2014	11/6/2014	Quorum: 87.53% Approval: 83.12%	Affirmative--10/31/14		
507	Project 2007-11	Project 2007-11 Disturbance Monitoring	Final Ballot	10/28/2014	11/6/2014	Quorum: 81.89% Approval: 68.51%	Affirmative--10/31/14		
508	Project 2007-11	Project 2010-05.2 Phase 2 of Special Protection Systems	Final Ballot	10/28/2014	11/6/2014	Quorum: 85.41% Approval: 73.33%	Negative--10/14/14		
509	Project 2007-11	Project 2009-03 Emergency Operations	Final Ballot	10/28/2014	11/6/2014	Quorum: 87.19% Approval: 73.20%	Affirmative--10/17/14		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
510	Project 2007-11	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Final Ballot	10/28/2014	11/6/2014	Quorum: 89.49%/87.66%/87.08 % Approval: 92.91%/92.15%/95.62 %	Affirmative--10/20/14		
511	Project 2014-03	Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions	Final Ballot	10/28/2014	11/6/2014	Quorum: 87.56%/87.32%87.07 %/87.56%/87.80%87.5 6%86.59% Approval: 83.84%/95.34%/86.00 %/95.35%91.17%/83.8 8%/95.40%/92.76%	CIP-003-6 no consensus CIP-010-2 no consensus New Definitions-Affirmative Updated Definitions-Affirmative Implementation Plan-Affirmative Version X Materials-Affirmative Non-binding polls-Affirmative		
512	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards	Additional Ballot	11/4/2014	11/10/2014	Quorum: 78.36% Approval: 60.21%	Affirmative--11/4/14		
513	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	Additional Ballot	11/12/2014	11/21/2014	Quorum: 79.73% Approval: 77.29%	Affirmative--11/21/14		
514	Project 2014-03	Project 2010-13.3 Phase 3 of Relay Loadability: Stable Power Swings	Additional Ballot	11/14/2014	11/24/2014	Quorum: 79.83% Approval: 67.39%	Affirmative--10/1/14		
515	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	Final Ballot	12/5/2014	12/16/2014	Quorum: 84.27% Approval: 78.05%	Affirmative--12/12/14		
516	Project 2014-03	Project 2010-13.3 Phase 3 of Relay Loadability: Stable Power Swings	Final Ballot	12/5/2014	12/16/2014	Quorum: 84.81% Approval: 68.08%	Affirmative--12/15/14		
517	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Initial Ballots	12/10/2014	12/23/2014	Quorum: 79.38%/79.72%/79.60 % Approval: 92.69%/93.55%/93.67 %	Affirmative--12/22/14		
518	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards	Additional Ballot	12/19/2014	1/7/2015	Quorum: 80.47% Approval: 72.43%	Affirmative--1/6/15		
519	Project 2014-02	2014-02 - Critical Infrastructure Protection Standards Version 5 Revisions	Additional Ballot	12/30/2014	1/9/2015	Quorum: 81.22%/81.71%/81.46 %/81.71%/81.71%/81. 22%/81.71%/81.46% Approval: 81.92%/98.89%/98.86 %/88.13%/98.89%/86. 02%/89.63%/97.21%	CIP-003-7 Binding and non-binding polls-no consensus CIP-003-7 Definition-Affirmative CIP-010-7 Binding and non-binding polls- Affirmative CIP-010-7 Definition- Affirmative CIP-004-7 Binding and non-binding polls – Affirmative CIP-007-7 Binding and non-binding polls –Affirmative CIP-011-7 Binding and non-binding polls –Affirmative CIP Implementation Plan- Affirmative 1/8/2015		
520	Project 2014-03	2014-03 - Revisions to TOP and IRO Standards - TOP-001-3	Final Ballots	1/15/2015	1/21/2015	Quorum: 84.70% Approval: 72.69%	Affirmative--1/6/15		
521	Project 2014-01	2014-01 - Standards Applicability for Dispersed Generation Resources - PRC-005-5	Initial Ballots	1/12/2015	1/22/2015	Quorum: 77.93% Approval: 93.74%	Affirmative--1/22/15		
522	Project 2014-01	2014-01 - Standards Applicability for Dispersed Generation Resources - PRC-001-1.1(iii), PRC-019-2, and PRC-024-2	Final Ballots	1/13/2015	1/22/2015	Quorum: 89.27%/89.30%/89.52 % Approval: 93.99%/94.03%/95.82 %	Affirmative--1/22/15		
523	Project 2014-02	2014-02 - Critical Infrastructure Protection Standards Version 5 Revisions CIP-003-7, CIP-004-7, CIP-010-3, and CIP-011-3	Final Ballot	1/23/2015	2/2/2015	Quorum: 84.15%/84.39%/84.15 %/84.39%/84.39%/83. 90%/84.39%/83.66% Approval: 79.76%/98.94%/98.94 %/86.76%/98.93%/84. 07%/90.10%/97.32%	Affirmative--1/29/15		
524	Project 2014-01	2014-01 - Standards Applicability for Dispersed Generation Resources - PRC-005-5	Final Ballot	3/2/2015	3/11/2015	Quorum: 83.52% Approval: 98.03%	Affirmative--1/22/15		
525	Project 2010-14.1	Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	Additional Ballot	3/6/2015	3/16/2015	Quorum: 77.29% Approval: 59.30%	Negative--3/13/2015		
526	Project 2008-02.2	Project 2008-02.2 Phase 2 of Undervoltage Load Shedding (UVLS): Misoperations	Initial Ballot	3/27/2015	4/7/2015	Quorum: 79.93% Approval: 84.31%	Affirmative--3/31/15		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
527	Project 2014-04	Project 2014-04 Physical Security	Initial Ballot	3/31/2015	4/9/2015	Quorum: 88.33% Approval: 89.95%	Affirmative--3/31/15		
528	Project 2008-02.2	Project 2008-02.2 Phase 2 of Undervoltage Load Shedding (UVLS): Misoperations	Final Ballot	4/17/2015	4/27/2015	Quorum: 84.86% Approval: 89.63%	Affirmative--3/31/15		
529	Project 2014-04	Project 2014-04 Physical Security	Final Ballot	4/20/2015	4/29/2015	Quorum: 92.00% Approval: 92.35%	Affirmative--3/31/15		
530	Project 2007-06	Project 2007-06 System Protection Coordination	Additional Ballot	5/6/2015	5/15/2015	Quorum: 81.79% Approval: 39.63%	Negative--5//13/15		
531	Project 2015-06	2015-06 Interconnection Reliability Operations and Coordination	Initial Ballot	6/29/2015	7/8/2015	Quorum: 75.23%/84.00% Approval: 90.35%/97.50%	Affirmative--7/7/15		
532	Project 2015-04	2015-04 Alignment of Terms	Initial Ballot	7/17/2015	7/27/2015	Quorum: 90.43%/91.17%/91.10 %/91.01%/91.10%/91. 17%/91.17%/91.34%/ 90.97%/91.40%/90.10 %/91.01%/91.07%/91. 07%/91.07%/91.34%/ 91.43%/90.75%/91.34 %/91.01%/91.40%/91. 01%/91.01%/91.01%// 91.01%/91.01% Approval: 91.46%/88.57%/86.68 %/97.06%/97.10%/81. 06%/80.73%/96.38%/ 97.03%/69.80%/95.38 %/93.62%/96.83%/97. 00%/98.55%/87.37%/ 89.99%/84.38%/88.06 %/90.37%/97.75%/91. 28%/87.71%/89.44%// 87.15%/98.24%	Affirmative--7/24/15		
533	Project 2015-06	2015-06 Interconnection Reliability Operations and Coordination	Final Ballots	7/22/2015	7/31/2015	Quorum: 85.98%/90.67%% Approval: 88.23%/96.84%	Affirmative--7/7/15		
534	Project 2010-14.1	Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	Additional Ballot	8/11/2015	8/20/2015	Quorum: 75.92% Approval: 69.26%	Affirmative--8/17/15		
535	Project 2007-06	Project 2007-06 System Protection Coordination	Additional Ballot	9/2/2015	9/11/2015	Quorum: 84.34% Approval: 69.76%	Affirmative--9/8/15		
536	Project 2007-06	Project 2007-06.2 Phase 2 of System Protection Coordination	Initial Ballot	9/2/2015	9/11/2015	Quorum: 87.16% Approval: 62.55%	Affirmative--9/11/15		
537	Project 2010-14.2.1	Project 2010-14.2.1 Phase 2 of Balancing Authority Reliability-based Controls – BAL-005 and BAL-006	Initial Ballot	9/4/2015	9/14/2015	Quorum: 83.81% Approval: 55.97%	Abstention--9/14/15		
538	Project 2015-04	2015-04 Alignment of Terms	Final Ballot	9/4/2015	9/14/2015	Quorum: 96.81%/97.53%/97.51 %/97.48%/97.51%/97. 53%/97.53%/97.11%// 97.11%/97.85%/96.80 %/97.12%/97.14%/97. 14%/97.14%/97.11%// 97.14%/96.80%/97.11 %/97.48%/97.85%/97. 48%/97.48%/97.48%// 97.48%/97.48%	Affirmative--7/24/15		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
						Approval: 93.13%/92.89%/91.33 %/98.07%/98.07%/84. 78%/84.75%/98.30%/ 98.06%/75.63%/95.46 %/94.48%/98.31%/97. 11%/98.57%/90.80%/ 95.60%/90.46%/92.07 %/92.49%/97.81%/92. 84%/91.09%/91.32%/ 90.80%/98.29%	Affirmative--7/24/15		
539	Project 2007-17.4	Project 2007-17.4 PRC-005 FERC Order No. 803 Directive	Initial Ballot	9/4/2015	9/16/2015	Quorum: 86.97%	Affirmative--9/16/15		
540	Project 2010-04.1	Project 2010-04.1 MOD-031 FERC Order No. 804 Directives	Initial Ballot	9/9/2015	9/18/2015	Approval: 96.73%	Affirmative--9/18/15		
541	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems: Remedial Action Schemes (RAS)	Initial Ballot	9/25/2015	10/5/2015	Quorum: 83.70%	N egative--10/2/15		
542	Project 2010-05.3	Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	Final Ballot	9/29/2015	10/8/2015	Approval: 48.10%	Affirmative--8/17/15		
543	Project 2010-05.3	Project 2007-06 System Protection Coordination	Final Ballot	10/5/2015	10/14/2015	Quorum: 84.28%	Affirmative--9/8/15		
544	Project 2010-05.3	Project 2010-04.1 MOD-031 FERC Order No. 804 Directives	Final Ballot	10/6/2015	10/15/2015	Approval: 74.61%	Affirmative--9/18/15		
545	Project 2007-17.4	Project 2007-17.4 PRC-005 FERC Order No. 803 Directive	Final Ballot	10/15/2015	10/26/2015	Quorum: 89.16%	Affirmative--9/16/15		
546	Project 2010-05.3	Project 2009-02 Real-time Reliability Monitoring and Analysis Capabilities	Initial Ballot	10/30/2015	11/9/2015	Approval: 80.94%	Abstention--11/5/15		
547	Project 2010-05.3	Project 2010-14.2.2 Phase 2 of Balancing Authority Reliability-based Controls - BAL-004-2	Initial Ballot	11/3/2015	11/12/2015	Quorum: 84.59%/84.49%	Affirmative--11/5/15		
548	Project 2015-07	Project 2015-07 Internal Communications Capabilities	Initial Ballot	11/6/2015	11/16/2015	Approval: 47.38%/48.00%	Affirmative--11/13/15		
549	Project 2007-06.2	Project 2007-06.2 Phase 2 of System Protection Coordination	Additional Ballot	11/10/2015	11/19/2015	Quorum: 88.18%	Affirmative--11/18/15		
550	Project 2010-07.1	Project 2010-07.1 Vegetation Management	Initial Ballot	12/7/2015	12/16/2015	Approval: 53.60%	Negative--12/8/15		
547	Project 2010-05.3	Project 2010-14.2.2 Phase 2 of Balancing Authority Reliability-based Controls - BAL-004-2	Final Ballot	12/8/2015	12/17/2015	Quorum: 83.18%	Affirmative--11/5/15		
551	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems: Remedial Action Schemes (RAS)	Additional Ballot	12/30/2015	1/8/2016	Approval: 57.29%	Affirmative--12/3015		
552	Project 2010-14.2.1	Project 2010-14.2.1 Phase 2 of Balancing Authority Reliability-based Controls -BAL-005 and BAL-006	Additional Ballot	12/31/2015	1/11/2016	Quorum: 83.39%/80.88%	BAL-005-1--Negative--1/10/16 BAL-006--Affirmative--1/10/16 FAC-003-1--Abstention--1/10/16		
553	Project 2010-05.3	Project 2009-02 Real-time Reliability Monitoring and Analysis Capabilities	Additional Ballot	1/15/2016	1/25/2016	Approval: 60.39%/92.94%	Affirmative--1/25/16		
554	Project 2010-07.1	Project 2010-07.1 Vegetation Management	Final Ballot	1/29/2016	2/8/2016	Quorum: 82.88%/82.18%	Affirmative--2/1/16		
552	Project 2010-14.2.1	Project 2010-14.2.1 Phase 2 of Balancing Authority Reliability-based Controls -BAL-005 and BAL-006	Final Ballot	1/29/2016	2/8/2016	Approval: 72.13%/68.01%	Affirmative--2/3/15		
551	Project 2010-05.3	Project 2009-02 Real-time Reliability Monitoring and Analysis Capabilities	Final Ballot	2/17/2016	2/26/2016	Quorum: 86.35%/86.98%/86.67 %	Affirmative--1/25/16		
552	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems: Remedial Action Schemes (RAS)	Additional Ballot	3/9/2016	3/18/2016	Approval: 75.68%/73.87%	Affirmative--3/10/16		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
553	Project 2007-06.2	Project 2007-06.2 Phase 2 of System Protection Coordination	Initial Ballot	4/15/2016	4/25/2016	Quorum: 83.39%/83.33% Approval: 80.57%/78.39%	Affirmative--4/20/16		
554	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems: Remedial Action Schemes (RAS)	Final Ballot	4/20/2016	4/29/2016	Quorum: 81.19%/87.15% Approval: 80.36%/93.43%	Affirmative--3/10/16		
555	Project 2015-07	Project 2015-07 Internal Communications Capabilities	Additional Ballot	4/27/2016	5/6/2016	Quorum: 81.03% Approval: 82.64%	Affirmative--5/6/16		
556	Project 2007-06.2	Project 2007-06.2 Phase 2 of System Protection Coordination	Final Ballot	5/17/2016	5/26/2016	Quorum: 88.96%/88.36% Approval: 82.52%/83.37%	Affirmative--4/20/16		
557	Project 2015-07	Project 2015-07 Internal Communications Capabilities	Final Ballot	6/15/2016	6/24/2016	Quorum: 84.52% Approval: 83.25%	Affirmative--5/6/16		
558	Project 2016-01	Project 2016-01 Modifications to TOP and IRO Standards	Initial Ballot	7/25/2016	8/3/2016	Quorum: 84.50%/85.51% Approval: 67.25%/64.59%	Affirmative--8/1/16		
559	Project 2015-08	Project 2015-08 Emergency Operations EOP-005-3 EOP-006-3 EOP-008-2	Initial Ballot	8/4/2016	8/15/2016	Quorum: 80.45%/81.14%/80.79 % Approval: 52.90%/66.87%/84.13 %	Negative--8/4/16		
560	Project 2016-02	Project 2016-02 Modifications to CIP Standards	Initial Ballot	8/26/2016	9/6/2016	Quorum: 85.00%/84.37%/84.62 % Approval: 41.54%/41.77%/30.63 %	Negative--9/6/16		
561	Project 2015-08	Project 2015-08 Emergency Operations EOP-004-4	Initial Ballot	8/30/2016	9/8/2016	Quorum: 82.75% Approval: 80.32%	Affirmative--9/8/16		
562	Project 2015-INT-01	Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)	Initial Ballot	9/2/2016	9/12/2016	Quorum: 75.43% Approval: 91.68%	Affirmative--9/12/16		
563	Project 2016-01	Project 2016-01 Modifications to TOP and IRO Standards	Additional Ballot	10/5/2016	10/14/2016	Quorum: 83.33%/81.79% Approval: 70.77%/68.85%	Affirmative--10/13/16		
564	Project 2015-INT-01	Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)	Final Ballot	10/13/2016	10/24/2016	Quorum: 81.25% Approval: 91.31%	Affirmative--9/12/16		
565	Project 2016-02	Project 2016-02 Modifications to CIP Standards	Additional Ballot	11/23/2016	12/5/2016	Quorum: 76.40%/76.63% Approval: 85.56%/75.54%	Affirmative--12/1/16		
566	Project 2015-08	Project 2015-08 Emergency Operations EOP-005-3 and EOP-006-3	Additional Ballot	11/30/2016	12/9/2016	Quorum: 80.71%/82.43% Approval: 76.93%/77.17%	Affirmative--11/30/16		
567	Project 2015-08	Project 2015-08 Emergency Operations EOP-008-2	Final Ballot	11/30/2016	12/9/2016	Quorum: 93.36% Approval: 93.17%	Affirmative--11/30/16		
568	Project 2016-01	Project 2016-01 Modifications to TOP and IRO Standards	Final Ballot	12/2/2016	12/12/2016	Quorum: 90.74%/90.40% Approval: 74.30%/72.52%	Affirmative--12/2/16		
569	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-7 and Implementation	Final Ballot	12/9/2016	12/19/2016	Quorum: 82.89%/83.14% Approval: 87.95%/83.03%	Affirmative--12/1/16		
570	Project 2015-08	Project 2015-08 Emergency Operations EOP-004-4	Additional Ballot	12/28/2016	1/6/2017	Quorum: 79.47% Approval: 93.55%	Affirmative--1/4/17		
571	Project 2015-08	Project 2015-08 Emergency Operations EOP-005-3, EOP-006-3	Final Ballot	12/28/2016	1/6/2017	Quorum: 91.00%/91.55% Approval: 83.65%/80.56%	Affirmative--1/4/17		
572	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan and 2 Definitions	Initial Ballot	1/16/2017	1/25/2017	Quorum: 77.81%/76.71%/77.26 %/76.71%	Affirmative--1/23/17		

Line	Project	Link to Ballot Results (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
						Approval: 81.30%/87.87%/86.75 %/86.47%	Affirmative--1/23/17		
573	Project 2016-03	Project 2016-03 Cyber Security Supply Chain Risk Management	Initial Ballot	2/24/2017	3/6/2017	Quorum: 87.13%	Abstain--3/2/17		
						Approval: 10.36%			
574	Project 2015-08	Project 2015-08 Emergency Operations EOP-004-4	Final Ballot	1/24/2017	2/2/2017	Quorum: 84.46%	Affirmative--1/4/17		
						Approval: 93.80%			
575	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan and 2 Definitions	Final Ballot	1/30/2017	2/8/2017	Quorum: 86.58%/85.48%/86.03 %/85.48%	Affirmative--1/23/17		
						Approval: 78.55%/86.00%/85.81 %/85.54%			
576	SPM	Revisions to the NERC Standards Process Manual	Initial Ballot	4/24/2017	5/3/2017	Quorum: 78.21%			
						Approval: 64.72%			
577	Project 2016-03	Project 2016-03 Cyber Security Supply Chain Risk Management	Additional Ballot	6/6/2017	6/15/2017	Quorum: 76.02%/76.02%/77.21 %	Affirmative--6/8/17		
						Approval: 89.84%/82.92%/88.64 %			
578	Project 2016-03	Project 2016-03 Cyber Security Supply Chain Risk Management	Final Ballot	7/11/2017	7/20/2017	Quorum: 81.59%/81.33%/82.84 %	Affirmative--6/8/17		
						Approval: 88.79%/81.40%/84.19 %			
579	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation TPL-007-2	Initial Ballot	8/2/2017	8/11/2017	Quorum: 79.87%	Affirmative--8/3/17		
						Approval: 72.67%			
580	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Initial Ballot	8/29/2017	9/8/2017	Quorum: 80.45%	Affirmative--9/1/17		
						Approval: 78.79%			
581	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1 Control Center Communication Networks	Initial Ballot	8/14/2017	9/12/2017	Quorum: 80.00%	Affirmative--9/1/17		
						Approval: 42.74%			
582	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Initial Ballot	9/8/2017	10/23/2017	Quorum: 82.71%	Abstain--10/18/17		
						Approval: 30.50%			
583	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation TPL-007-2	Final Ballot	10/20/2017	10/30/2017	Quorum: 88.74%	Affirmative--8/3/17		
						Approval: 73.35%			
584	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Initial Ballot	9/14/2017	10/30/2017	Quorum: 85.40%	Affirmative--10/30/17		
						Approval: 66.78%			
585	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Initial Ballot	11/3/2017	11/13/2017	Quorum: 87.01%/86.90%/86.90 %/85.57%/85.85	Affirmative--11/10/17		
						Approval: 58.12%/63.17%/56.55 %/76.40%/68.59%			
586	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1	Additional Ballot	11/20/2017	12/11/2017	Quorum:77.10%	Affirmative--12/4/17		
						Approval: 63.91%			
587	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Additional Ballot	10/30/2017	12/13/2017	Quorum: 81.73%	Affirmative--12/4/17		
						Approval: 88.25%			
588	Project 2016-04	Project 2016-04 Modifications to PRC-025-1	Final Ballot	1/9/2018	1/18/2018	Quorum: 82.69%	Affirmative--12/4/17		
						Approval: 89.46%			
589	Project 2017-02	Project 2017-02 Modifications to Personnel Performance, Training and Qualifications	Initial Ballot	2/26/2018	3/7/2018	Quorum: 80.93%/81.27%	Affirmative--3/2/18		
						Approval: 97.50%/98.91%			
590	Project 2017-02	Project 2017-02 Modifications to Personnel Performance, Training and Qualifications	Final Ballot	4/3/2018	4/12/2018	Quorum: 84.82%/84.86%	Affirmative--3/2/18		
						Approval: 96.64%/97.88%			
591	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Additional Ballot	2/23/2018	4/23/2018	Quorum: 80%	Affirmative--4/16/18		
						Approval: 26.44%			
592	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Additional Ballot	3/16/2018	4/30/2018	Quorum: 79.50%	Affirmative--4/25/18		
						Approval: 93.31%			
593	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1	Additional Ballot	3/16/2018	4/30/2018	Quorum:78.06%	Affirmative--4/25/18		
						Approval: 83.71%			
594	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1 Control Center Definition and Implementation Plan	Initial Ballot	3/16/2018	4/30/2018	Quorum: 81.33%/81.54%	Negative--4/25/18		
						Approval: 46.71%/37.98%			
595	Project 2017-06	Project 2017-06 Modifications to BAL-002-2	Initial Ballot	4/27/2018	5/8/2018	Quorum: 81.82%	Abstain--5/7/17		
						Approval: 80%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
596	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1	Additional Ballot	5/18/2018	7/3/2018	Quorum: 75.16% Approval: 68.45%	Affirmative--6/29/18		
597	Project 2017-06	Project 2017-06 Modifications to BAL-002-2	Final Ballot	7/5/2018	7/16/2018	Quorum: 84.42% Approval: 71.85%	Abstain--5/7/17		
598	SPM	Revisions to the NERC Standards Process Manual	Additional Ballot	7/31/2018	8/9/2018	Quorum: 80.34% Approval: 81.95%	Affirmative--8/7/18		
599	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-012-1	Final Ballot	8/3/2018	8/13/2018	Quorum:81.55% Approval: 72..55%	Affirmative--4/25/18		
600	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Additional Ballot	9/5/2018	9/14/2018	Quorum: 75.59% Approval: 69.07%	Affirmative--9/5/18		
601	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Initial Ballot	9/28/2018	10/9/2018	Quorum: 78.59% Approval: 55.89%	Affirmative--10/5/18		
602	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-8	Initial Ballot	9/28/2018	10/9/2018	Quorum: 78.77% Approval: 90.06%	Affirmative--10/5/18		
603	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Additional Ballot	10/8/2018	10/17/2018	Quorum: 83.65%/84.08%/83.77 %/84.82%/82.43%/82. 11%/84.08%/83.60%/ 83.12%/80.98%/83.28 % Approval: 67.65%/67.46%/53.22 %/77.07%/59.02%/59. 79%/75.07%/69.27%// 71.98%/69.93%/82.26 %	Affirmative--10/12/18		
604	Project 2018-02	Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting	Initial Ballot	10/18/2018	10/22/2018	Quorum: 81.17% Approval: 20.02%	Reject--10/22/18		
605	Project 2015-10	Project 2015-10 Single Points of Failure TPL-001	Final Ballot	10/11/2018	10/22/2018	Quorum: 86.39% Approval: 66.69%	Affirmative--9/5/18		
606	SPM	Revisions to the NERC Standards Process Manual	Final Ballot	10/7/2018	10/29/2018	Quorum: 85.96% Approval: 81.61%	Affirmative--8/7/18		
607	Project 2018-01	Project 2018-01 Canadian-specific Revisions to TPL-007-2	Initial Ballot	11/6/2018	11/15/2018	Quorum: 77.54%/79.10% Approval: 100%/100%	Affirmative--11/6/18		
608	Project 2018-02	Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting	Additional Ballot	11/20/2018	11/29/2018	Quorum: 94.44% Approval: 75.54%	Affirmative--11/20/18		
609	Project 2018-01	Project 2018-01 Canadian-specific Revisions to TPL-007-2	Final Ballot	11/29/2018	12/10/2018	Quorum: 80.43%/82.09% Approval: 100%/100%	Affirmative--11/6/18		
610	Project 2017-01	Project 2017-01 Modifications to BAL-003-1.1	Initial Ballot	1/8/2019	1/17/2019	Quorum: 92.02%/91% Approval: 96.41%/99.04%	Affirmative--1/14/19		
611	Project 2018-02	Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting	Final Ballot	1/15/2019	1/22/2019	Quorum: 96.30% Approval: 77.89%	Affirmative--11/20/18		
612	Project 2018-03	Project 2018-03 Standards Efficiency Review Retirements	Initial Ballot	4/3/2019	4/12/2019	Quorum: 86.75%/87.96%/87.80 %/87.58%/87.58%/87. 50%/87.58%/87.34%// 87.46%/86.45%/87.34 %/86.77%/87.17%/87. 17%/86.89%/85.71%// 85.67%/86.39% Approval: 96.18%/98.88%/97.41 %/97.79%/98.51%/89. 75%/98.53%/96.60%// 95.96%/96.60%/95.80 %/98.95%/96.45%/96. 54%/95.90%/88.42%// 98.96%/97.69%	Affirmative--4/10/19 for all standards except three. Negative--4/10/19 on following standard: PRC-004-5(i), INT-010-2.1 and FAC-0008-3		
613	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-003-8	Final Ballot	4/18/2019	4/29/2019	Quorum: 83.64% Approval: 91.44%	Affirmative--10/5/18		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
614	Project 2018-03	Project 2018-03 Standards Efficiency Review Retirements	Final Ballot	4/3/2019	4/12/2019	Quorum: 90.22%/90.97%/90.85 %/90.94%/90.94%/90. 88%/90.60%/90.26%/ 90.43%/90.32%/90.26 %/90.65%90.13%/90.1 3%/89.84%/90.06%/9 0.03%/89.56% Approval: 95.74%/86.66%/85.94 %/96.64%/97.22%/90. 19%/97.19%/95.47%/ 94.63%/94.34%/94.69 %/96.59%95.28%/95.4 1%94.55%/87.12%/97. 75%/96.57%	Affirmative--4/10/19 for all standards except three.		
615	Project 2018-04	Project 2018-04 Modifications to PRC-024-2	Initial Ballot	5/22/2019	5/31/2019	Quorum: 88.08% Approval: 52.28%	Abstain--5/29/19		
616	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Additional Ballot	6/3/2019	7/17/2019	Quorum: 85.40% Approval: 87.39%	Affirmative--7/15/19		
617	Project 2019-01	Project 2019-01 Modifications to TPL-007-3	Initial Ballot	8/30/2019	9/9/2019	Quorum: 91.44% Approval: 88.81%	Affirmative--9/5/19		
618	Project 2017-01	Project 2017-01 Modifications to BAL-003-1.1	Final Ballot	10/10/2019	10/24/2019	Quorum: 92.96% Approval: 1001%	Affirmative--1/14/19		
619	Project 2018-04	Project 2018-04 Modifications to PRC-024-2	Additional Ballot	10/25/2019	11/4/2019	Quorum: 81.88% Approval: 86.67%	Affirmative--11/4/19		
620	Project 2019-01	Project 2019-01 Modifications to TPL-007-3	Final Ballot	11/13/2019	11/22/2019	Quorum: 94.52% Approval: 78.95%	Affirmative--9/5/19		
621	Project 2017-07	Project 2017-07 Standards Alignment with Registration	Initial Ballot	12/3/2019	12/12/2019	Quorum: 88.76%/89.02%/89.02 %/88.98%/89.96%/89. 06%/88.72%/87.89% Approval: 99.69%/99.36%/99.69 %/99.69%/99.59%/99. 38%/99.69%/99.68%	Affirmative--12/12/19		
622	Project 2018-04	Project 2018-04 Modifications to PRC-024-2	Final Ballot	12/4/2019	12/13/2019	Quorum: 89.26% Approval: 82.47%	Affirmative--11/4/19		
623	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Additional Ballot	11/1/2019	12/16/2019	Quorum: 81.89% Approval: 95.98%	Affirmative--12/12/19		
624	Technical Rationale for Reliability Standards	Technical Rationale for Reliability Standards	Non-binding Poll	12/9/2019	12/18/2019	Quorum: 85.46%/82.52%/82.83 %/82.35%/82.76%/86. 55%/81.77%/86.82%/ 82.76% Approval: 84.91%/88.89%/85.12 %/86.57%/86.57%/86. 79%/89.55%/88.75%/ 77.78%	Affirmative--12/12/19		
625	Project 2017-07	Project 2017-07 Standards Alignment with Registration	Final Ballot	1/14/2020	1/23/2020	Quorum: 89.53%/89.8%/89.8%/ 89.76%/90.83%/89.84 %/89.88%/88.67% Approval: 99.69%/99.69%/99.69 %/99.69%/99.6%/99.3 8%/99.69%/99.69%	Affirmative--12/12/19		
626	Project 2019-02	Project 2019-02 BES Cyber System Information Access Management	Initial Ballot	1/24/2020	2/3/2020	Quorum: 92.09%/92.78%/91.58 % Approval: 15.37%/13.04%/22.30 %	Abstain--1/31/20		
627	Project 2019-03	Project 2019-03 Cyber Security Supply Chain Risks	Initial Ballot	1/27/2020	3/11/2020	Quorum: 88.37% Approval: 50.51%	Abstain--2/26/20		
628	Project 2016-02	Project 2016-02 Modifications to CIP Standards CIP-002-6	Final Ballot	3/26/2020	4/6/2020	Quorum: 87.92% Approval: 96.28%	Affirmative--12/12/19		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
629	Technical Rationale for Reliability Standards	Technical Rationale for Reliability Standards	Non-binding Poll	4/10/2020	4/20/2020	Quorum: 81.93%/82.24%/80.49 %/82.17%/81.44%/81. 78%/81.3%/81.92%/8 0.93%/81.73% Approval: 86.475/87.77%/87.12 %/85.48%/85.7%/87.1 %/86.93%/85.8%/76.9 %/79.25%	Affirmative--4/17/20		
630	Project 2019-03	Project 2019-03 Cyber Security Supply Chain Risks	Additional Ballot	6/12/2020	6/22/2020	Quorum: 78.74% Approval: 34.44%	Abstain--2/26/20		
631	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Initial/Additional Ballot	7/24/2020	8/26/2020	Quorum: 81.48%/81.73%/81.35 %/81.15%/80.57%/80. 98%/80.43%/80.67%/ 91.18%/91.48% Approval: 58.50%/88.32%/79.26 %/86.98%/72.82%/88. 78%/88.50%/89.16%/ 85.21%/81.17%	Affirmative--7/24/20		
632	Project 2019-02	Project 2019-02 BES Cyber System Information Access Management	Additional Ballot	9/11/2020	9/21/2020	Quorum: 84.98%/83.82%/82.84 % Approval: 32.80%/23.06%/50.49 %	Abstain--9/17/20		
633	Project 2019-03	Project 2019-03 Cyber Security Supply Chain Risks	Final Ballot	10/7/2020	10/16/2020	Quorum: 83.56% Approval: 76.76%	Abstain--2/26/20		
634	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Additional Ballot	11/27/2020	12/7/2020	Quorum: 82.82%/82.41% Approval: 66.61%/89.79%	Affirmative--12/4/20		
635	Project 2018-03	Project 2018-03 Standards Efficiency Review Retirements	Initial Ballot	4/3/2019	4/12/2019	Quorum: 89.93%/86.61% Approval: 95.91%/100%	Affirmative--1/4/21		
636	Project 2018-03	Project 2018-03 Standards Efficiency Review Retirements	Final Ballot	1/19/2021	1/28//21	Quorum: 91.04% Approval: 95.96%	Affirmative--1/4/21		
637	Project 2019-06	Project 2019-06 Cold Weather	Initial Ballot	3/3/2021	3/12//21	Quorum: 89.71%/89.49%/89.81 % Approval: 49.39%/66.22%/64.35 %	Affirmative--3/3/21		
638	Project 2016-02	Project 2016-02 Modifications to CIP Standards Virtualization	Initial Ballot	3/12/2020	3/22/2021	Quorum: 90.26%/89.94%/89.87 %/89.87%/89.87%/90. 16%/89.87%/89.54%/ 89.87%.89.54%.89.54 % Approval: 38.87%/48.30%/51.17 %/26.30%/42.81%/42. 32%/52.87%/53.26%/ 32.43%/47.25%/51.23 %	Abstain--3/17/21		
639	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Additional Ballot	2/19/2021	4/5/2021	Quorum: 80.67% Approval: 92.35%	Affirmative--3/31/21		
640	Project 2019-06	Project 2019-06 Cold Weather	Additional Ballot	4/2/2021	4/26//21	Quorum: 87.74%/86.58%/86.26 % Approval: 77.10%/85.42%/85.20 %	Affirmative--3/3/21		
641	Project 2015-09	Project 2015-09 Establish and Communicate System Operating Limits	Final Ballot	4/29/2021	5/10/2021	Quorum: 85.76%/83.44%/86.19 %/86.45%/85.67%/86. 19%/94.42%/94.00%/ 84.57%	Affirmative--3/31/21		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
						Approval: 82.83%/92.34%/93.75 %/94.17%/93.55%/94. 18%/89.59%/87.93%/ 93.01%	Affirmative--3/31/21		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
1.	N/A	Standards Project Prioritization Reference Document and Tool	Project Prioritization Tool		1/21/11	2/10/11	Yes 2/10/11
2.	Project 2007-23	Project 2007-23 - Violation Severity Levels	VSLs		1/20/11	2/18/11	Yes 2/18/11
3.	N/A	CAN-0015--Draft CAN-0015 Unavailability of NERC Tools	CAN-0015 Unavailability of NERC Tools		2/4/11	2/18/11	Yes 2/18/11
4	N/A	CAN-0016--Draft CAN-0016 CIP-001-1 R1 - Applicability to Non-BES	CAN-0016 CIP-001-1, R1		2/4/11	2/18/11	Yes 2/18/11
5.	N/A	CAN-0018--Draft CAN-0018 FAC-008 R.1.2.1 - Terminal Equipment	CAN-0018 FAC-008, R.1.2.1		2/4/11	2/18/11	Yes 2/18/11
6.	Regional Standard	Regional Reliability Standards - PRC-006-NPCC-1 - Automatic Underfrequency Load Shedding	PRC-006-NPCC-1		1/10/11	2/24/11	
7.	Project 2007-07	Project 2007-07 - Vegetation Management - FAC-003	FAC-003-2		1/27/11	2/28/11	Yes 2/28/11
8.	N/A	CAN-0017--Draft CAN-0017 CIP-007 R5 System Access and Password Controls	CAN-0017 CIP-007, R5		2/11/11	3/4/11	Yes 3/4/11
9.	Project 2007-12	Project 2007-12 - Frequency Response	BAL-003-1		2/4/11	3/7/11	Yes 3/7/11
10.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	COM-001 COM-002 IRO-001 IRO-014		1/18/11	3/7/11	Yes 3/7/11
11.	NERC RoP	Proposed Changes to Rules of Procedure to Add Section 1700 - Challenges to Determinations	RoP Section 1700		2/14/11	3/7/11	Yes 3/7/11
12.	Project 2009-02	Project 2009-02 - Real-time Reliability Monitoring and Analysis Capabilities	Concept White Paper		2/16/11	4/4/11	Yes 4/4/11

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
13.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR Standards		3/4/11	4/4/11	<u>Yes 4/4/11</u>
14.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		3/9/11	4/8/11	<u>Yes 4/8/11</u>
15.	RFC RoP	Notice of Proposed Changes to RFC Rules of Procedure and Request for Comments			3/1/11	4/15/11	
16.	NERC RoP	Proposed Amendments to NERC Rules of Procedure Appendices 3B and 3D	Appendices 3B and 3D		3/1/11	4/15/11	<u>Yes 4/15/11</u>
17.	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3 - CIP-005	CIP-005		3/29/11	4/28/11	<u>Yes 4/27/11</u>
18.	Project 2009-06	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	FAC-008-3		3/17/11	5/2/11	<u>Yes 5/2/11</u>
19.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		4/13/11	5/12/11	<u>Yes 5/9/11</u>
20.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		4/28/11	5/27/11	<u>Yes 5/27/11</u>
21.	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs	TPL-001-2		4/18/11	5/31/11	<u>Yes 5/31/11</u>
22.	Project 2007-03	Project 2007-03 - Real-time Operations - TOP-001 through TOP-008 and PER-001	TOP-001 through TOP-008 and PER-001		4/26/11	6/9/11	<u>Yes 6/9/11</u>
23.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		5/11/11	6/10/11	<u>Yes 6/10/11</u>
24.	NERC RoP	Rules of Procedure Development Team: BES Definition Exception Process	BES Definition Exception Process		5/11/11	6/10/11	<u>Yes 6/10/11</u>

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
25.	N/A	CAN-0024--Draft CAN-0024 CIP-002 through CIP-009 Routable Protocols and Data Diodes	CAN-0024 CIP-002 through CIP- 009		5/20/11	6/10/11	
26.	N/A	CAN-0029--Draft CAN-0029 PRC- 004-1 R1, R2 and R3 Misoperations	CAN-0029 PRC-004- 1 R1, R2 and R3		5/20/11	6/10/11	
27.	N/A	CAN-0030--Draft CAN-0030 Attestations	CAN-0030 Attestations		5/20/11	6/10/11	
28.	N/A	CAN-0039--Draft CAN-0039 DOE Form 407	CAN-0039 DOE Form 407		5/20/11	6/10/11	
29.	Project 2010-05.1	Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations)			6/10/11	7/11/11	
30.	Project 2007-09	Project 2007-09 – Generator Verification – MOD- 025-2, MOD-027-1, PRC-019-1	MOD-025-2 MOD-027-1 PRC-019-1		6/15/11	7/15/11	Yes 7/15/11
31.	Project 2010-07	Project 2010-07 – Generator Requirements at the Transmission Interface – Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR standards	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR standards		6/17/11	7/17/11	Yes 7/15/11
32.	Project 2007-09	Project 2007-09 – Generator Verification – MOD- 026-1 and PRC-024- 1	MOD-026-1 and PRC-024-1		6/15/11	8/1/11	Yes 8/1/11
33.	NERC RoP	Proposed Changes to NERC Rules of Procedure and associated Appendices (Appendix 4B – Sanction Guidelines; and Appendix 4C – Compliance Monitoring and Enforcement Program)	Appendices 4B and 4C		6/30/11	8/15/11	
34.	N/A	Compliance Application Notice (CAN) Process	CAN Process		8/15/11	9/6/11	Yes 9/6/11

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
35..	N/A	CAN-0016 CIP-001 R1 - Sabotage Reporting Procedure	CAN-0016 CIP-001, R1		8/15/11	9/6/11	Yes 9/6/11
36.	N/A	DRAFT CANs Posted for Comment and Retirement of CAN-0001 through 0004	CAN-0001 through 0004 Retirement		8/31/11	9/21/11	
37.	NERC RSDP	NERC 2012-2014 Reliability Standards Development Plan	2012-2014 RSDP		9/12/11	9/26/11	Yes 9/26/11
38.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		8/15/11	9/28/11	Yes 9/28/11
39.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Definition of BES	BES Definition		8/26/11	10/10/11	Yes 10/10/11
40.	Project 2010-17	Project 2010-17 - Bulk Electric System (BES) Definition - Technical Principles for Demonstrating BES Exceptions	Technical Principles for Demonstrating BES Exceptions		8/26/11	10/10/11	Yes 10/10/11
41.	N/A	New CAN Template, five DRAFT CANs for Industry review and CANs Status posted to NERC Compliance's Web site.	CANs		9/23/11	10/14/11	Yes 10/14/11
42.	RoP	Proposed Changes to NERC Rules of Procedure and All Appendices			9/2/11	10/17/11	
43.	Project 2010-17	Project 2010-17 - Bulk Electric System (BES) Definition - Rules of procedure Modifications to Support BES Exception Requests	RoP Section 509, Section 1703 and Appendix 5C		9/13/11	10/27/11	Yes 10/27/11
44.	N/A	CAN-0010--Definition of "Annual" and Implementation of Annual Requirements	CAN-0010 Definition of Annual		10/10/11	10/31/11	Yes 10/31/11

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
45.	N/A	CAN-0011--PRC-005-1 R2: New Equipment	CAN-0011 PRC-005-1 R2		10/10/11	10/31/11	Yes 10/31/11
46.	N/A	CAN-0012-- Completion of Periodic Activity Requirements During Implementation Plan	CAN-0012 Completion of Periodic Activity Requirements		10/10/11	10/31/11	Yes 10/31/11
47	N/A	CAN-0013--PRC-023 R1 and R2 Effective Dates for Switch-on-to-Fault Schemes	CAN-0013 PRC-023 R1 and R2		10/10/11	10/31/11	
48.	N/A	CAN-0015-- Unavailability of NERC Software Tools	CAN-0015 NERC Tools		10/10/11	10/31/11	Yes 10/31/11
49.	N/A	CAN-0022--VAR-002-1.1b R1 and R3 Generator Operation in Manual Mode	CAN-0022 VAR-002-1.1b R1 and R3		10/10/11	10/31/11	
50.	N/A	CAN-0024--CIP-002 R3 Routable Protocols and Data Diode Devices	CAN-0024 CIP-002, R3		10/10/11	10/31/11	Yes 10/31/11
51.	N/A	CAN-0026--TOP-006 R3 Protection Relays	CAN-0026 TOP-006, R3		10/10/11	10/31/11	Yes 10/31/11
52.	N/A	CAN-0028--TOP-006-1 R1.2 Reporting Responsibilities	CAN-0028 TOP-006-1, R1.2		10/10/11	10/31/11	
53.	N/A	CAN-0020--TPL-002, TPL-003, TPL-004 and TOP-002 Equipment Maintenance Outages	CAN-0020 TPL-002, TPL-003, TPL-004 and TOP-002		10/19/11	11/9/11	
54.	N/A	CAN-0030-- Attestations	CAN-0030		10/19/11	11/9/11	
55.	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	MOD-028, R3.1		10/3/11	11/16/11	Yes 11/16/11
56.	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Interpretation of COM-002-2, R2		10/4/11	11/18/11	Yes 11/18/11

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
57.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR Standards		10/5/11	11/18/11	Yes 11/18/11
58.	N/A	Draft Directive Regarding Generator Transmission Leads	Draft Directive #2011 CAG-001		10/17/11	11/18/11	Yes 11/18/11
59.	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-1 R1.1 by Progress Energy	Interpretation of CIP-006-1, R1.1		10/12/11	11/21/11	Yes 11/21/11
60.	N/A	CAN-0040 - BAL-003 Frequency Bias Calculation			11/2/11	11/23/11	
61.	N/A	CAN-0043 - PRC-005 Protection System Maintenance and Testing Evidence	PRC-005 Evidence		11/2/11	11/23/11	Yes 11/22/11
62.	Project 2007-12	Project 2007-12 - Frequency Response	BAL-003-1			12/8/11	Yes 12/8/11
63.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2			12/12/11	Yes 12/12/11
64.	N/A	Draft CAN-0027: TOP-003 R2 Coordination of Scheduled Outages	CAN-0027 TOP-003, R2		11/22/11	12/14/11	
65.	NERC RoP	Proposed Changes to the NERC Rules of Procedure and Associated Appendices			11/7/11	12/22/11	
66.	NERC RoP	Notice of Revisions to Proposed New Sections 1.1.24 and 5.11 of Appendix 4C of the NERC Rules of Procedure, as Originally Posted for Comment on November 7, 2011			11/22/11	12/22/11	
67.	Regional Standard	Regional Reliability Standard PRC-006-NPCC-1 — Automatic Underfrequency Load Shedding	PRC-006-NPCC-1		11/22/11	12/22/11	

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
68.	Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1 (Version 5 CIP Standards)	Version 5 CIP Standards		11/7/11	1/6/12	Yes 1/6/12
69.	Project 2007-03	Project 2007-03 - Real-time Transmission Operations - TOP-001-2, TOP-002-3 and TOP-003-2	TOP-001-2 TOP-002-3 TOP-003-2		12/14/11	1/12/12	Yes 1/12/12
70.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	BES Definition, Phase 2		1/4/12	2/3/12	Yes 2/3/12
71.	N/A	Order 754 - Request for Data or Information	Data Request		12/22/11	2/6/12	Yes 2/6/12
72.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002 and IRO-001-3	COM-001 COM-002 IRO-001-3		1/9/12	2/9/12	Yes 2/8/12
73.	WECC Regional Standard	Regional Reliability Standard BAL-004-WECC-02 - Automatic Time Error Correction	BAL-004-WECC-02		1/23/12	3/9/12	
74.	WECC Regional Standard	Regional Reliability Standard BAL-001-0.1a - Real Power Balancing Control Performance - WECC Variance	BAL-001-0.1a		1/23/12	3/9/12	
75.	N/A	NERC Functional Model Demand Response Functions and Entities	NERC Functional Model		2/13/12	3/14/12	
76.	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 for WECC	Interpretation of CIP-004-1		2/8/12	3/23/12	Yes 3/23/12
77.	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Interpretation of CIP-002-1, R3		2/8/12	3/23/12	Yes 3/23/12

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
78.	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR -002 for Constellation	Interpretation of VAR -002		2/8/12	3/23/12	Yes 3/23/12
79.	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing - PRC-005	PRC-005-2		2/28/12	3/28/12	Yes 3/28/12
80.	Project 2007-09	Project 2007-09 Generator Verification - MOD-026-1 and PRC-024-1	MOD-026-1 and PRC-024-1		2/29/12	3/29/12	Yes 3/29/12
81.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface - FAC-003-X, FAC-003-3	FAC-003-X FAC-003-3		3/9/12	4/9/12	Yes 4/9/12
82.	Project 2007-09	Project 2007-09 Generator Verification - MOD-025-2, MOD-027-1, and PRC-019-1	MOD-025-2 MOD-027-1 PRC-019-1		2/29/12	4/16/12	Yes 4/16/12
83.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface - PRC-005-1.1a	PRC-005-1.1a		3/2/12	4/16/12	Yes 4/16/12
84.	Project 2007-03	Project 2007-03 - Real-time Transmission Operations	TOP-001 through TOP-008 and PER-001		3/22/12	4/20/12	Yes 4/20/12
85.	Project 2012-INT-02	Request for Interpretation - Project 2012-INT-02 TPL-003-0a and TPL-004-0 for SPCS	Interpretation of TPL-003-0a and TPL-004-0		4/24/12	5/4/12	
86.	Project 2008-06	Project 2008-06 - Cyber Security Order 706 Version 5 CIP	CIP-002 and CIP-003 - Comment Form A		4/12/12	5/21/12	Yes 5/20/12
			CIP-004 thru CIP-007 - Comment Form B		4/12/12	5/21/12	Yes 5/20/12
			CIP-008 thru CIP-011 - Comment Form C		4/12/12	5/21/12	Yes 5/20/12
			Definitions and Implementation Plan - Comment Form D		4/12/12	5/21/12	Yes 5/20/12
87.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		4/25/12	5/24/12	Yes 5/24/12

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
88.	Project 2007-12	Project 2007-12 Frequency Response Technical Conferences			5/30/12	6/15/12	
89.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	COM-003		5/7/12	6/20/12	<u>Yes 6/20/12</u>
90.	N/A	Adequate Level of Reliability Revised Definition and Associated Documents	Adequate Level of Reliability (ALR)		4/25/12	6/25/12	<u>Yes 6/25/12</u>
91.	N/A	Order 754 - Request for Data or Information	Data Request		5/11/12	6/25/12	<u>Yes 6/25/12</u>
92.	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR -002 for Constellation	Interpretation of VAR -002		5/22/12	6/27/12	<u>Yes 6/27/12</u>
93.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		5/29/12	6/27/12	<u>Yes 6/27/12</u>
94.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserve	BAL-001-1		6/4/12	7/3/12	<u>Yes 7/3/12</u>
			BAL-002-2		6/4/12	7/3/12	<u>Yes 7/3/12</u>
			BAL-012-1		6/4/12	7/3/12	<u>Yes 7/3/12</u>
			BAL-013-1		6/4/12	7/3/12	<u>Yes 7/3/12</u>
95.	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-001 and PRC-027		5/21/12	7/5/12	<u>Yes 7/5/12</u>
96.	N/A	Cost Effective Analysis Process (CEAP) for NERC ERO Standards	CEAP		5/7/12	7/6/12	<u>Yes 7/6/12</u>
97.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002 and IRO-001-3	COM-001, COM-002 and IRO-001-3		6/7/12	7/6/12	<u>Yes 7/6/12</u>
98.	Project 2006-02	Project 2006-02 – Assess Transmission Future Needs and Develop Transmission Plans	TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12		6/19/12	7/9/12	<u>Yes 7/9/12</u>

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
99.	N/A	Standard Processes Manual Revisions to Implement SPIG Recommendations	SPIG Reco		6/20/12	7/19/12	Yes 7/19/12
100.	Project 2012-INT-02	Project 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for System Protection and Control Subcommittee	- Interpretation of TPL-003-0a and TPL-004-0		6/20/12	7/20/12	Yes 7/19/12
101.	Project 2012-INT-05	Interpretation of 2012-INT-05 - Interpretation of CIP-002-3 for OGE	Interpretation of CIP-002-3		6/27/12	7/27/12	Yes 7/27/12
102.	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision to Address Interpretation of VAR-002 for Constellation	Rapid Revision to VAR-002		7/18/12	7/27/12	Yes 7/26/12
103.	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Rapid Revision of TOP-006		6/14/12	7/30/12	Yes 7/27/12
104.	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Glossary of Terms		6/19/12	8/2/12	Yes 8/2/12
105.	N/A	Reliability Guideline: System Operator Verbal Communications – Current Industry Practices	System Operator Verbal Communications		6/26/12	8/10/12	Yes 8/9/12
106.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		7/27/12	8/27/12	Yes 8/27/12
107.	Project 2010-11	Project 2010-11 - TPL Table 1 Order TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12	TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12		7/31/12	8/29/12	Yes 8/29/12
108.	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs			7/31/12	8/30/12	
109.	Project 2009-19	Project 2009-19 – Interpretation of BAL-002 by NWPP Reserve Sharing Group			7/25/12	9/4/12	

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
110.	Project 2013-02	Project 2013-02 - Paragraph 81	Paragraph 81		8/3/12	9/4/12	Yes 9/4/12
111.	Project 2010-05.1	Project 2010-05.1 - Protection Systems: Phase 1 (Misoperations)			7/25/12	9/7/12	Yes 9/7/12
112.	N/A	Definition of Adequate Level of Reliability	Adequate Level of Reliability (ALR)		8/15/12	9/13/12	Yes 9/13/12
113.	N/A	2013-2015 Reliability Standards Development Plan	2013-2015 RSDP		8/17/12	9/18/12	Yes 9/18/12
114.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols	COM-003-1		8/22/12	9/20/12	Yes 9/20/12
115.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		8/29/12	9/27/12	
116.	SPP Regional Standard	Regional Reliability Standard PRC-006-SPP-01 Automatic Underfrequency Load Shedding	PRC-006-SPP-01		8/15/12	9/28/12	
117.	Project 2008-06 Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1	Version 5 CIP Standards		9/11/12	10/10/12	Yes 10/10/12
			RSAP		9/11/12	10/10/12	Yes 10/10/12
118.	MRO SPM	Regional Reliability Standards - MRO Standards Process Manual			8/28/12	10/11/12	
119.	N/A	Standard Process Manual Revisions to Implement SPIG Recommendations	SPIG Reco		8/29/12	10/12/12	Yes 10/10/12
120.		Revisions to Outstanding VRFs and VSLs			9/5/12	10/19/12	
121.	Project 2013-01	Project 2013-01 - Cold Weather Preparedness			9/25/12	10/24/12	
122.	Project 2007-09	Project 2007-09 - Generator Verification			9/28/12	10/29/12	
123.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System			10/4/12	11/5/12	
124.	2007-12	Project 2007-12 - Frequency Response			10/5/12	11/7/12	

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
125.	Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1	Version 5 CIP Standards		10/26/12	11/7/12	
126.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	PRC-025		10/5/12	11/7/12	
127.	N/A	IRO-006-WECC-2			10/3/12	11/16/12	
128.	Project 2010-11	Project 2010-11 - TPL Table 1, Footnote B			10/5/12	11/19/12	
129.	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Interpretation of TPL-003-0a and TPL-004-0		10/22/12	12/5/12	Yes 12/5/12
130.	Project 2013-02	Project 2013-02 - Paragraph 81	Paragraph 81		10/25/12	12/10/12	Yes 12/10/12
131.	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	- Interpretation of CIP-003-3		11/9/12	12/10/12	Yes 12/10/12
132.	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	- Interpretation of CIP-007-3		11/9/12	12/10/12	Yes 12/10/12
133.	Project 2007-02	Project 2007-02 - Operating Personnel Communication Protocols - RSAW	COM-003-1		11/14/12	12/13/12	Yes 12/13/12
			COM-003-1 RSAW		11/14/12	12/13/12	Yes 12/13/12
134.	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-001 and PRC-027		11/16/12	12/17/12	Yes 12/17/12
135.	Project 2012-INT-05	Project 2012-INT-05 - Interpretation of CIP-002-3 for OGE	Interpretation of CIP-002-3		11/6/12	12/20/12	Yes 12/20/12
136.	N/A	Standard Processes Manual to Implement SPIG Revisions	SPIG Reco		11/21/12	12/20/12	Yes 12/20/12
137.	Project 2010-11	Project 2010-11 - TPL Table 1, Footnote B	TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12		12/10/12	1/11/13	Yes 1/11/13
138.	Project 2007-09	Project 2007-09 - Generator Verification - PRC-024-1	PRC-024-1		12/12/12	1/11/13	Yes 1/11/13

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
139.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-012-1	BAL-012-1		11/30/12	1/14/13	Yes 1/14/13
140.	N/A	Reliability Guideline--Draft Generating Unit Winter Weather Readiness - Current Industry Practices			12/20/12	2/4/13	Yes 2/4/13
141.	Project 2010-05-1	Project 2010-05-1 Protection System Misoperations					Yes 2/20/13
142.	Project 2007-09	Project 2007-09 Generator Verification - PRC-024-1	PRC-024-1	Formal	1/25/13	2/25/13	Yes 2/25/13
143.	N/A	Rapid Revision Procedure		Informal	2/25/13	3/6/13	Yes 3/6/13
144.	Project 2010-13-2	Project 2010-13-2 - Phase 2 of Relay Loadability - Generation - PRC-025-1	PRC-025-1	Formal	1/25/13	3/11/13	Yes 3/11/13
			Supplemental SAR	Informal	1/25/13	3/11/13	Yes 3/11/13
			Cost Effectiveness	CEAP Pilot	1/25/13	3/11/13	Yes 3/11/13
			RSAA	Feedback	1/25/13	3/11/13	Yes 3/11/13
145.	Project 2012-INT-04	Interpretation 2012-INT-04 - Interpretation of CIP-007 for ITC	Interpretation of CIP-007	Formal	2/6/13	3/22/13	Yes 3/22/13
146.	Project 2012-INT-06	Interpretation 2012-INT-06 - Interpretation of CIP-003 for Consumers Energy	Interpretation of CIP-003	Formal	2/6/13	3/22/13	Yes 3/22/13
147.	Project 2012-08-1	Project 2012-08-1 - Phase 1 of Glossary Updates--Statutory Definitions	Glossary of Terms	Formal	2/21/13	3/22/13	Yes 3/22/13
148.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003-1	COM-003-1	Formal	3/7/13	4/5/13	Yes 4/5/13
			RSAA	Feedback	3/7/13	4/5/13	Yes 4/5/13
149.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves	BAL-001-2	Formal	3/12/13	4/25/13	Yes 4/25/13
			BAL-002-2	Formal	3/12/13	4/25/13	Yes 4/25/13
			BAL-013-1	Formal	3/12/13	4/25/13	Yes 4/25/13

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
150.	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays)	Draft SAR	Informal	4/5/13	5/6/13	Yes 5/6/13
			PRC-005-3	Formal	4/5/13	5/6/13	Yes 5/6/13
151.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation	PRC-023-3 PRC-025-1	Formal	4/25/13	5/24/13	Yes 5/24/13
152.	Project 2007-11	Project 2007-11 - Disturbance Monitoring — PRC-002 and PRC-018	SAR	Informal	5/03/13	6/03/13	Yes 6/3/13
153.	Project 2007-11	Project 2007-11 - Disturbance Monitoring PRC-002 and PRC-018	Request for Information	Informal	6/05/13	7/05/13	
154.	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	PRC-001 and PRC-027		6/04/13	7/03/13	Yes 7/03/13
155.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	BES Definition		5/29/13	7/12/13	Yes 7/12/13
156.	TRE Regional Standard	Regional Reliability Standard - BAL-001-TRE-01	BAL-001-TRE-01		5/31/13	7/15/13	
157.	N/A	NPCC Regional Standards Process Manual	NPCC RSPM		6/06/13	7/22/13	
158.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	COM-003-1		6/20/13	7/19/13	Yes 7/19/13
159.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	PRC-025-1		6/20/13	7/19/13	Yes 7/19/13
160.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023	PRC-023-3	Formal	6/20/13	8/05/13	Yes 8/5/13
161.	N/A	SPP RE Regional Standards Process Manual	SPP RSPM		6/26/13	8/09/13	
162.	Project 2013-03	Project 2013-03 - Geomagnetic Disturbance Mitigation	EOP-010-1	Formal	6/27/13	8/12/13	Yes 8/12/13

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
163.	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005	PRC-005-3	Formal	7/10/13	8/23/13	Yes 8/23/13
164.	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards	INT-004-3 INT-006-4 INT-009-2 INT-010-2 INT-011-1	Informal	7/25/13	8/23/13	Yes 8/23/13
165.	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	MOD-001-2	Formal	7/11/13	8/26/13	Yes 8/26/13
166.	Project 2010-01	Project 2010-01 - Training - PER-005-2	PER-005-2	Formal	7/19/13	9/03/13	Yes 9/3/13
167.	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	VAR-001-4 VAR-002-3	Formal	7/19/13	9/03/13	Yes 9/3/13
168	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	MOD-032-1 MOD-033-1	Formal	7/22/13	9/04/13	Yes 9/4/13
169.	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	MOD-031-1	Formal	7/22/13	9/04/13	Yes 9/4/13
170	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System – Phase 2	BES Definition Phase 2	Formal	8/6/13	9/4/13	Yes 9/4/13
171	Project 2012-13	Project 2012-13 - NUC Five-Year Review	NUC-001-2	5-year review	7/26/13	9/9/13	Yes 9/9/13
172	2014-2016 RSDP	2014-2016 Reliability Standards Development Plan	Reliability Standards Development Plan	Annual Review	8/30/13	9/13/13	Yes 9/13/13
173	Project 2010-02	Project 2010-02 Five-Year Review of FAC Standards	FAC-001-1 FAC-002-1	5-year review	8/1/13	9/16/13	Yes 9/16/13
174	Project 2010-02	Project 2010-02 Five-Year Review of FAC Standards	FAC-003-3 FAC-008-3 FAC-010-2.1 FAC-011-2 FAC-013-2 FAC-014-2	5-year review	8/1/13	9/16/13	Yes 9/16/13

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
175	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	BAL-002-2	Formal	8/2/13	9/16/13	Yes 9/16/13
176	Project 2009-03	Project 2009-03 — Five-Year Review of Emergency Operations EOP-001, EOP-002, EOP-003, and IRO-001	EOP-001-2.1b EOP-002-3.1 EOP-003-2	5-year review	8/6/13	9/19/13	Yes 9/19/13
177	Project 2012-09	Project 2012-09 IRO Five-Year Review	IRO-003-2 IRO-004-2 IRO-005-4 IRO-006-5 IRO-006-East IRO-008-1 IRO-009-1 IRO-010-1a	5-year review	8/7/13	9/20/13	Yes 9/20/13
178	Project 2008-02	Project 2008-02 Undervoltage Load Shedding	Revised SAR	Informal	9/10/13	10/9/13	Yes 10/9/13
179	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	EOP-010-1	Formal	9/4/13	10/18/13	Yes 10/18/13
180	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition	Formal	9/27/13	10/28/13	Yes 10/28/13
181	Project 2007-02	Project 2007-02 Operating Personnel Communications Protocols	COM-002-4	Formal	10/21/13	11/7/13	Yes 11/4/13
182	Project 2010-01	Project 2010-01 Training	PER-005-2	Formal	9/27/13	11/12/13	Yes 11/12/13
183	Project 2008-12	Project 2008-12 Coordinate Interchange Standards	Various INT Standards	Formal	9/30/13	11/13/13	Yes 11/13/13
184	Project 2012-05	Project 2012-05 ATC Revisions (MOD A)	MOD-001-2	Formal	10/4/13	11/20/13	Yes 11/18/13
185	Project 2010-03	Project 2010-03 Modeling Data (MOD B)	MOD-032-1, MOD-033-1	Formal	10/07/13	11/20/13	
186	Project 2010-04	Project 2010-04 Demand Data (MOD C)	MOD-031-1	Formal	10/09/13	11/22/13	Yes 11/22/13
187	Project 2013-04	Project 2013-04 Voltage and Reactive Control	VAR-001-4, VAR-002-3	Formal	10/11/13	11/25/13	Yes 11/25/13

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
188	Project 2009-03	Project 2009-03 Emergency Operations	SAR	Informal	11/06/13	12/05/13	Yes 12/5/13
189	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves	BAL-002-2	Formal	10/28/13	12/11/13	Yes 12/11/13
190	Project 2007-11	Project 2007-11 - Disturbance Monitoring	PRC-002-2	Formal	11/01/13	12/16/13	Yes 12/16/13
191	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-027	Formal	11/04/13	12/18/13	Yes 12/18/13
192	Project 2014-01	Project 2014-01 - Standards Applicability for Dispersed Generation Resources	SAR	Formal	11/20/13	12/19/13	Yes 12/19/13
193	Project 2010-01	Project 2010-01 Training - PER-005-2	PER-005-2	Formal	12/4/13	1/22/14	Yes 1/17/14
194	Project 2010-03	Project 2010-03 Modeling Date - MOD B	MOD-033-1	Formal	12/6/13	1/22/14	Yes 1/21/14
195	Project 2008-12	Project 2008-12 Coordinate Interchange Standards	INT-004-3 INT-010-2	Formal	1/10/14	1/24/14	Yes 1/22/14
196	Project 2007-02	Project 2007-02 Operating Personnel	COM-002-4	Formal	1/22/14	1/31/14	Yes 1/31/14
197	Project 2014-02	Project 2014-02 Standard Authorization Request – Cyber Security Standards	CIP SAR	Informal	1/17/14	2/18/14	Yes 2/18/14
198	2014 Work Plan	2014 Work Plan for NERC Reliability Standards Development	2014 Work plan			2/21/13	Yes 2/21/14
199	Project 2010-17	Project 2010-17 Definition of Bulk Electric System - Phase 2	BES	Informal	1/29/14	2/27/14	Yes 2/27/14
200	Project 2010-05.1	Project 2010-05.1 Protection System: Phase 1 (Misoperations) - PRC-004-3	PRC-004-3	Formal	1/17/14	3/11/14	Yes 3/2/14

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
201	Project 2012-13	Project 2012-13 NUC-Nuclear Plant Interface Coordination Standard Authorization Request	NUC-001-2.1 SAR	Informal	2/12/14	3/13/14	Yes 3/13/14
202	Project 2010-05.2	Project 2010-05.2 Special Protection Systems (Phase 2 of Protection Systems) - SAR	SAR	Informal	2/18/14	3/19/14	Yes 3/19/14
203	Project 2014-03	Project 2014-03 - Revisions to TOP/IRO Reliability Standards	SAR	Formal	02/21/14	03/24/14	Yes 3/24/14
204	Project 2014-03	Technical Conferences on Revisions to TOP/IRO Reliability Standards	Technical Conference Topics	Informal	03/11/14	03/24/14	
205	Project 2014-04	Project 2014-04 - Physical Security	SAR	Informal	03/21/14	03/28/14	Yes 3/28/14
206	Project 2010-14.2	Project 2010-14.2 - Periodic Review of BAL Standards	Reco to Revise BAL-005 and BAL-006	Formal	02/21/14	04/07/14	
207	2010-05.2	Project 2010-05.2 - Phase 2 of Protection Systems - Revised Definition of Special Protection System	SPS Definition	Informal	03/11/14	04/09/14	Yes 4/9/14
208	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	MOD-031-1	Formal	02/25/14	04/10/14	Yes 4/10/14
209	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	VAR-002-3	Formal	02/27/14	04/14/14	Yes 4/14/14
210	Project 2008-02	Project 2008-02 - Undervoltage Load Shedding - PRC-010, PRC-020, PRC-021 and PRC-022	PRC-010-1	Informal	03/17/14	04/16/14	Yes 4/16/14
211	Project 2014-04	Project 2014-04 Physical Security - CIP-014-1	CIP-014-1	Formal	04/10/14	04/24/14	Yes 4/24/14
212	Project 2009-03	Project 2009-03 Emergency Operations – EOP-011-1	EOP-011-1	Informal	03/28/14	04/28/14	Yes 4/28/14

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
213	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	PRC-005-2(X) PRC-005-3(X) PRC-005-X(X) VAR-002-2b(X) VAR-002-4	Formal	04/17/14	05/05/14	Yes 5/5/14
214	Project 2010-02	Project 2010-02 – Connecting New Facilities to the Grid	FAC-001-1 FAC-002-1	Formal	04/01/14	05/15/14	Yes 5/15/14
215	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	TPL-007-1	Informal	04/22/14	05/21/14	Yes 5/21/14
216	Project 2012-13	Project 2012-13 Nuclear Plant Interface Coordination	NUC-001-3	Formal	04/08/14	05/22/14	Yes 5/22/14
217	Project 2007-17.3	Project 2007-17.3 Protection System Maintenance and Testing – Phase 3 (Sudden Pressure Relays)	PRC-005-X	Formal	04/17/14	06/03/14	Yes 6/3/14
218	Project 2010-13.3	Project 2010-13.3 Relay Loadability: Stable Power Swings	PRC-026-1	Formal	04/25/14	06/09/14	Yes 6/9/14
219	Project 2007-11	Project 2007-11 Disturbance Monitoring	PRC-002-2	Formal	05/09/14	06/25/14	Yes 6/25/14
221	Project 2008-02	Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding	PRC-010 PRC-020 PRC-021 PRC-022	Informal	05/23/14	06/23/14	Yes 6/23/14
222	Project 2010-05-1	Project 2010-05-1 Protection System – Phase 1 – Misoperations	PRC-004	Formal	05/16/14	07/09/14	Yes 7/9/14
223	Project 2014-03	Project 2014-03 Revisions to TOP-IRO Reliability Standards	TOP-001-3 TOP-002-4 TOP-003-3 IRO-001-4 IRO-002-4 IRO-008-2 IRO-010-2 IRO-014-3 IRO-017-1	Formal	05/19/14	07/02/14	Yes 7/2/14
224	Project 2014-02	Project 2014-02 CIP Version 5 Revisions	CIP-002 to CIP-011	Formal	06/02/14	07/17/14	Yes 7/16/14

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		– Cyber Security Standards					
225	Project 2015-2017	Project 2015-2017 Reliability Standard Development Plan		Informal		7/21/14	Yes 7/21/14
226	2010-05.2	Project 2010-05.2 - Phase 2 of Protection Systems - Revised Definition of Special Protection System	SPS Definition	Formal	7/16/14	7/25/14	Yes 7/25/14
227	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	PRC-005-2(X) PRC-005-3(X) PRC-005-X(X) VAR-002-2b(X) VAR-002-4	Formal	06/12/14	7/29/14	Yes 7/29/14
228	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	TPL-007-1	Formal	06/13/14	07/30/14	Yes 7/30/14
229	Project 2008-02	Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding	PRC-010 PRC-020 PRC-021 PRC-022	Formal	06/23/14	08/8/14	Yes 8/6/14
230	Project 2010-14-2	Project 2010-14-2 Balancing Authority Reliability-based Control Standard Authorization Request for BAL-005 and BAL-006	BAL-005 BAL-006	Informal	07/16/14	08/14/14	Yes 8/12/14
231	Project 2009-03	Project 2009-03 Emergency Operations – EOP-011-1	EOP-011-1	Formal	07/2/14	08/15/14	Yes 8/13/14
232	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	PRC-004-2.1a(X) PRC-004-3(X)	Formal	07/10/14	08/26/14	Yes 8/25/14
233	Project 2007-17.3	Project 2007-17.3 Protection System Maintenance and Testing – Phase 3 (Sudden Pressure Relays) – PRC-005-X	PRC-005-X	Formal	07/30/14	09/12/14	Yes 9/12/14
234	Project 2014-03	Project 2014-03 Revisions to TOP-	TOP-001-3 TOP-002-4	Formal	08/6/14	09/19/14	Yes 9/22/14

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		IRO Reliability Standards	TOP-003-3 IRO-001-4 IRO-002-4 IRO-008-2 IRO-010-2 IRO-014-3 IRO-017-1				
235	Project 2010-14.1	Project 2010-14.1 Balancing Authority Reliability-based Control	BAL-002-2	Formal	08/19/14	10/03/14	Yes 10/2/14
236	Project 2010-13.3	Project 2010-13.3 – Relay Loadability: Stable Power Swings	PRC-026-1	Formal	09/26/14	10/06/14	Yes 10/6/14
237	Project 2008-02	Project 2008-02: Underfrequency Load Shedding (UFLS)	PRC-006-2	Formal	08/21/14	10/08/14	Yes 10/7/14
238	Project 2013-03	Project 2013-03: Geomagnetic Disturbance Mitigation	TPL-007-1	Formal	08/27/14	10/10/14	Yes 10/10/14
239	NERC Rules of Procedure	NERC Rules of Procedure	NERC Rules of Procedure	Formal	08/26/14	10/10/14	Yes 10/14/14
240	Project 2010-05.2	Project 2010-05.2 – Special Protection Systems Phase 2 of Protection Systems	RAS Definition	Formal	08/29/14	10/14/14	Yes 10/14/14
241	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	VAR-002-2b(X) VAR-002-4	Formal	08/27/14	10/16/14	Yes 10/16/14
242	Project 2014-02	Project 2014-02 CIP Version 5 Revisions – Cyber Security Standards	CIP-003-6 CIP-010-2 CIP-003-X CIP-004-X CIP-007-X CIP-010-X CIP-011-X	Formal	09/03/14	10/17/14	Yes 10/17/14
243	Project 2009-03	Project 2009-03 Emergency Operations	EOP-011-1	Formal	09/05/14	10/20/14	Yes 10/20/14
244	Project 2007-06	Project 2007-06 System Protection Coordination PRC-027-1 (Preliminary Draft 5)	PRC-027-1	Informal	10/01/14	10/21/14	Yes 10/21/14

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
245	Project 2007-11	Project 2007-11 Disturbance Monitoring	PRC-002-2	Formal	09/05/14	10/21/14	Yes 10/21/14
246	Project 2014-01	Project 2014-01 Applicability for Dispersed Generation	PRC-004-2.1a(X) PRC-004-4	Formal	09/05/14	10/22/14	Yes 10/22/14
247	Project 2014-03	Project 2014-03 Revisions to TOP/IRO Reliability Standards TOP-001-3	TOP-001-3	Formal	10/10/14	11/10/14	Yes 11/10/14
248	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation TPL-007-1	TPL-007-1	Formal	10/28/14	11/21/14	Yes 11/24/14
249	Project 2010-13.3	Project 2010-13.3 – Relay Loadability: Stable Power Swings	PRC-026-1	Formal	11/04/14	11/24/14	Yes 11/25/14
250	Project 2014-01	Project 2014-01 – Standards Applicability for Dispersed Generation Resources	PRC-001-1.1 PRC-019-2 PRC-024-1	Formal	11/05/14	12/23/14	Yes 12/22/14
251	Project 2014-03	Project 2014-03 Revisions to TOP/IRO Reliability Standards TOP-001-3	TOP-001-3	Formal	12/29/14	1/7/15	Yes 1/6/15
252	Project 2014-02	Project 2014-02 CIP Version 5 Revisions	CIP-003-7 CIP-004-7 CIP-007-7 CIP-010-3 CIP-011-3 CIP-003-7 CIP-010-3 Implementation Plan	Formal	12/30/14	1/9/15	Yes 1/9/15
253	Project 2014-04	Project 2014-04 Physical Security SAR	SAR	Informal	12/15/14	1/13/15	Yes 1/12/15
254	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	White Paper Appendix A Appendix B	Informal	12/22/14	1/20/15	Yes 1/20/15
255	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed	PRC-005-5	Informal	12/22/14	1/20/15	Yes 1/22/15

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		Generation Resources					
257	Project 2010-14.1	Project 2010-14.1 Balancing Authority Reliability-based Control	BAL-002-2	Formal	1/29/15	3/18/15	Yes 3/16/15
258	Reliability Guideline	Reliability Guideline: Loss of Real-Time Reliability Tools Capability/Loss of Equipment Significantly Affecting ICCP Data		Formal	2/19/15	4/6/15	Yes 4/6/15
259	Project 2008-02.2	Project 2008-02.2 Phase 2 UVLS: Misoperation	PRC-010-2	Formal	2/20/15	4/7/15	Yes 4/7/15
260	Project 2014-04	Project 2014-04 Physical Security	CIP-014-2	Formal	2/20/15	4/9/15	Yes 4/9/15
261	Project 2015-04	Project 2015-04 Alignment of Terms	SAR	Formal	2/24/15	4/13/15	Yes 4/13/15
262	Project 2007-17.4	Project 2007-17.4 PRC-005 Order No. 803 Directives	SAR	Informal	3/12/15	4/10/15	Yes 4/13/15
263	Project 2015-06	Project 2015-06 Interconnection Reliability Operations and Coordination	SAR	Informal	3/16/15	4/15/15	Yes 4/15/15
264	Project 2010-14.2.2	Project 2010-14.2.2 Phase 2 of Balancing Authority Reliability-based Controls: Time Error Correction	SAR	Informal	3/17/15	4/15/15	Yes 4/15/15
265	Project 2015-02	Project 2015-02 Periodic Review of Emergency Operations	EOP-008-1	Informal	3/27/15	5/11/15	Yes 5/11/15
266	Project 2015-02	Project 2015-02 Periodic Review of Emergency Operations	EOP-006-2	Informal	3/27/15	5/11/15	Yes 5/11/15
267	Project 2015-02	Project 2015-02 Periodic Review of Emergency Operations	EOP-005-2	Informal	3/27/15	5/11/15	Yes 5/11/15
268	Project 2015-02	Project 2015-02 Periodic Review of Emergency Operations	EOP-004-2	Informal	3/27/15	5/11/15	Yes 5/11/15

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
269	Project 2007-06	Project 2007-06 System Protection Coordination PRC-027-1 (Draft 5)	PRC-027-1	Formal	4/1/15	5/15/15	Yes 5/15/15
270	Project 2010-04.1	Project 2010-04.1 MOD-031 FERC Order No. 804 Directives	SAR	Informal	4/16/15	5/19/15	Yes 5/19/15
271	Project 2010-05.3	Project 2010-05.3 Phase 3 of Protection Systems – RAS	PRC-012-2	Informal	4/30/15	5/20/15	Yes 5/20/15
272	Project 2015-03	Project 2015-03 Periodic Review of System Operating Limit Standards	FAC-010-3 FAC-011-3 FAC-014-2	Formal	5/4/15	6/17/15	Yes 6/17/15
273	Project 2015-06	Project 2015-06 Interconnection Reliability Operations and Coordination	IRO-006-East-2 IRO-009-2	Formal	5/21/15	7/8/15	Yes 7/8/15
274	Project 2007-17.4	Project 2007-17.4 PRC-005 FERC Order No. 803 Directive	PRC-005-3	Formal	6/11/15	7/10/15	Yes 7/10/15
275	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generations Resources	PRC-004-2.1 PRC-005-2 PRC-005-3	Informal	6/12/15	7/13/15	Yes 7/13/15
276	Project 2015-07	Project 2015-07 Internal Communications Capabilities	COM-001-2	Informal	6/11/15	7/15/15	Yes 7/15/15
277	Project 2015-04	Alignment of Terms	Glossary Terms	Formal	6/12/15	7/23/15	Yes 7/23/15
278	Project 2009-02	Real-time Monitoring and Analysis Capabilities	SAR	Formal	7/16/15	8/17/15	Yes 8/17/15
279	NERC 2016-2018	Reliability Standards Development Plan	Development Plan	Formal	7/16/15	8/17/15	Yes 8/17/15
280	Project 2015-08	Emergency Operations	EOP-004-2 EOP-005-2 EOP-006-2 EOP-008-1	Informal	7/21/15	8/19/15	Yes 8/19/15
281	Project 2010-14.1	Phase 1 of Balancing Authority Reliability-based Controls	BAL-002-2	Formal	7/7/15	8/20/15	Yes 8/20/15
282	Project 2010-	Phase 2 of Balancing Authority	BAL-004-0	Survey	8/12/15	8/25/15	Yes 8/25/15

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
	14.2.2	Reliability-based Controls: Time Error Correction					
283	Project 2007-06.2	Phase 2 of System Protection Coordination	TOP-009-1	Formal	7/29/15	9/11/15	Yes 9/11/15
284	Project 2007-06	System Protection Coordination	PRC-027-1	Formal	7/29/15	9/11/15	Yes 9/11/15
285	Project 2010-14.2.1	Phase 2 of Balancing Authority Reliability-based Controls	BAL-005-1 BAL-006-3	Formal	7/30/15	9/14/15	Yes 9/14/15
286	Project 2007-17.4	PRC-005 FERC Order No. 803 Directive	PRC-005-6	Formal	7/30/15	9/16/15	Yes 9/16/15
287	Project 2010-04.1	MOD-031 FERC Order No. 804 Directives	MOD-031-2	Formal	7/31/15	9/18/15	Yes 9/18/15
288	Project 2015-09	Establish and Communicate System Operating Limits	FAC-010-3 FAC-011-3 FAC-014-2	Informal	8/20/15	9/21/15	Yes 9/21/15
289	Project 2010-07.1	Vegetation Management	FAC-003-3	Informal	8/24/15	9/28/15	Yes 9/28/15
290	Project 2010-05.3	Phase 3 of Protection Systems: Remedial Action Schemes	PRC-012-2	Formal	8/20/15	10/5/15	Yes 10/5/15
291	Project 2009-02	Real-time Reliability Monitoring and Analysis Capabilities	IRO-018-1 TOP-010-1	Formal	9/24/15	11/9/15	Yes 11/9/15
292	Project 2010-14.2.2	Phase 2 of Balancing Authority Reliability-based Controls	BAL-004-0	Formal	9/24/15	11/12/15	Yes 11/12/15
293	Project 2015-07	Internal Communications Capabilities	COM-001-3	Formal	9/25/15	11/16/15	Yes 11/16/15
294	Project 2007-06.2	Phase 2 of System Protection Coordination	TOP-009-1	Formal	10/6/15	11/19/15	Yes 11/19/15
295	Project 2010-07.1	Vegetation Management	FAC-003-3	Formal	10/30/15	12/16/15	Yes 12/16/15
296	Project 2015-10	Single Points of Failure SAR	TPL-001	Informal	11/12/15	12/17/15	Yes 12/17/15
297	Project 2010-05.3	Phase 3 of Protection Systems RAS	PRC-012-2	Formal	11/25/15	1/8/16	Yes 1/8/16
298	Project 2010-14.2.1	Phase 2 of Balancing Authority Reliability-based Controls	BAL-005-1 FAC-001-3 BAL-006-2	Formal	12/31/15	1/11/16	Yes 1/11/16

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
299	Project 2009-02	Real-time Reliability Monitoring and Analysis Capabilities	IRO-018-1 TOP-010-1	Formal	12/10/15	1/25/16	Yes 1/25/16
300	Project 2016-01	Modifications to TOP and IRO Standards	SAR	Informal	1/22/16	2/22/16	Yes 2/22/16
301	Project 2010-05.3	Phase 3 of Protection Systems RAS	PRC-012-2	Formal	2/3/16	3/18/16	Yes 3/18/16
302	Project 2016-02	Modifications to CIP Standards	SAR	Informal	3/23/16	4/21/16	Yes 4/21/16
303	Project 2007-06.2	Phase 2 of System Protection Coordination	PER-006-1 & Two Definitions	Formal	3/10/16	4/25/16	Yes 4/25/16
304	Project 2015-07	Internal Communications Capabilities	COM-001-3	Formal	3/23/16	5/9/16	Yes 5/6/16
305	CEP	Cost Effectiveness Pilot	TPL-001-4	Informal	4/27/16	5/26/16	Yes 5/26/16
306	Project 2013-03	Geomagnetic Disturbance Mitigation Revised White Papers	SAR	Informal	5/12/16	6/13/16	Yes 6/13/16
307	Project 2015-10	Single Points of Failure	SAR	Informal	5/26/16	6/24/16	Yes 6/24/16
308	Project 2016-02	Modifications to CIP Standards	SAR	Informal	6/1/16	6/30/16	Yes 6/30/16
309	Draft 2017-2019	Reliability Standards Development Plan	RSDP	Informal	6/20/16	7/19/16	Yes 7/19/16
310	EPR	Enhanced Periodic Review Standing Review Team	Standards Grading	Informal	6/30/16	8/1/16	Yes 8/1/16
311	Project 2016-01	Modifications to TOP and IRO Standards	IRO-002-5 TOP-001-4	Formal	6/20/16	8/3/16	Yes 8/3/16
312	Project 2015-09	Establish and Communicate System Operating Limits	FAC-014-3	Formal	7/14/16	8/12/16	Yes 8/12/16
313	Project 2015-09	Establish and Communicate System Operating Limits	FAC-011-4	Formal	7/14/16	8/12/16	Yes 8/12/16
314	Project 2015-08	Emergency Operations	EOP-005-3 EOP-006-3 EOP-008-2	Formal	6/30/16	8/15/16	Yes 8/15/16
315	Project 2016-02	Modifications to CIP Standards	CIP-003-7	Formal	7/21/16	9/6/16	Yes 9/6/16
316	FMAG	Functional Model Advisory Group	Reliability Functional Model and Technical Document	Informal	7/21/16	9/7/16	Yes 9/7/16
317	Project	Emergency	EOP-004-4	Formal	7/25/16	9/8/16	Yes 9/8/16

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
	2015-08	Operations					
318	Project 2015-INT-01	Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)	CIP-002-5.1	Formal	7/27/16	9/12/16	Yes 9/12/16
319	Project 2016-01	Modifications to TOP and IRO Standards SAR	TOP-001-3 IRO-002-4	Formal	8/31/16	10/17/16	Yes 10/14/16
320	Project 2016-04	Modifications to PRC-025-1 SAR	PRC-025-1	Formal	9/16/16	10/18/16	Yes 10/18/16
321	Project 2016-03	Cyber Security Supply Chain Management	SAR	Informal	10/20/16	11/18/16	Yes 11/18/16
322	Project 2016-02	Modifications of CIP Standards	CIP-003-TCA	Informal	11/1/16	11/18/16	Yes 11/18/16
323	Project 2016-02	Modifications of CIP Standards	CIP-003-7	Formal	11/23/16	12/5/16	Yes 12/5/16
324	Project 2015-08	Emergency Operations	EOP-005-3 EOP-006-3	Formal	10/26/16	12/9/16	Yes 12/9/16
325	Project 2015-08	Emergency Operations	EOP-004-4	Formal	11/18/16	1/6/17	Yes 1/6/17
326	Project 2013-03	Geomagnetic Disturbance Mitigation	SAR	Informal	12/16/16	1/20/17	Yes 1/20/17
327	Project 2016-02	Modifications of CIP Standards	CIP-003-7(i)	Formal	12/12/16	1/25/17	Yes 1/25/17
328	Project 2016-EPR-01	Enhanced Periodic Review of Personnel Performance, Training and Qualifications Standard (PER)	PER-001-0.2 PER-003-1 PER-004-2	Formal	1/10/17	2/23/17	Yes 2/23/17
329	Project 2016-03	Cyber Security Supply Chain Risk Management	CIP-013-1	Formal	1/19/17	3/6/17	Yes 3/6/17
330	Project 2016-04	Modifications to PRC-025-1	SAR	Informal	3/20/17	4/3/17	Yes 4/3/17
331	Project 2016-02	Modifications to CIP Standard	Virtualization	Informal	3/14/17	4/11/17	Yes 4/11/17
332	Project 2016-02	Modifications to CIP Standard	TOCC	Informal	3/14/17	4/11/17	Yes 4/11/17
333	Project 2016-EPR-02	Enhanced Periodic Review of Voltage and Reactive (VAR) Standards	VAR-001-4.1	Formal	2/28/17	4/13/17	Yes 4/13/17
334	Project 2016-EPR-02	Enhanced Periodic Review of Voltage and Reactive (VAR) Standards	VAR-002-4	Formal	2/28/17	4/13/17	Yes 4/13/17
335	SPM	Revisions to the NERC Standard	SPM	Formal	3/20/17	5/3/17	Yes 5/3/17

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		Processes Manual					
336	Project 2015-10	Single Points of Failure	TPL-001-5	Informal	4/25/17	5/24/17	Yes 5/24/17
337	Project 2016-03	Cyber Security Supply Chain Risk Management	CIP-005-6 CIP-010-3 CIP-013-1	Formal	5/2/17	6/15/17	Yes 6/15/17
338	Project 2017-01	Modifications to BAL-003-1.1 SAR	BAL-003-1.1	Formal	6/19/17	7/18/17	Yes 7/18/17
339	Project 2017-06	Modifications to BAL-002-2 SAR	BAL-002-2	Informal	6/20/17	7/20/17	Yes 7/20/17
340	Project 2017-02	Modifications to Personnel Performance, Training and Qualifications Standards	PER-003-1 PER-004-2	Informal	6/21/17	7/24/17	Yes 7/24/17
341	2018-2010	Reliability Standards Development Plan		Formal	6/22/17	7/25/17	Yes 7/26/17
342	Standards Grading	Periodic Review Standing Review Team	Standards Grading	Informal	6/19/17	8/2/17	Yes 8/2/17
343	Project 2013-03	Geomagnetic Disturbance Mitigation	TPL-007-2	Formal	6/28/17	8/11/17	Yes 8/11/17
344	Project 2017-07	Alignment with Registration	Registration	Formal	8/1/17	8/30/17	Yes 8/30/17
345	Project 2017-07	Alignment with Registration	MOD-032-1 SAR	Formal	8/1/17	8/30/17	Yes 8/30/17
346	Reliability Guideline	Area Control Error Diversity Interchange Process	ACE Process	Formal	7/18/17	8/31/17	Yes 8/31/17
347	Project 2016-04	Modifications to PRC-025-1	PRC-025-2	Formal	7/25/17	9/7/17	Yes 9/7/17
348	Project 2016-02	Modifications to CIP Standard	CIP-012-1	Formal	7/27/17	9/11/17	Yes 9/11/17
349	Project 2016-02	Modifications to CIP Standard	Technical Rationale and Justification for CIP-012-1	Informal	8/14/17	9/12/17	Yes 9/12/17
350	Project 2016-02	Modifications to CIP Standard	Definition of Control Center	Informal	8/14/17	9/12/17	Yes 9/12/17
351	Project 2015-10	Single Points of Failure	TPL-001-5	Formal	9/8/17	10/23/17	Yes 10/23/17
352	Project 2016-02	Modifications to CIP Standard	CIP-002-6	Formal	9/14/17	10/30/17	Yes 10/30/17
353	Project 2015-09	Establish and Communicate System Operating Limits	Proposed Definitions of System Operating Limit (SOL) and SOL Exceedance	Informal	9/29/17	10/30/17	Yes 10/30/17
354	Project 2016-02	Modifications to CIP Standard	Virtualization	Informal	10/6/17	11/2/17	Yes 11/2/17
355	Project 2015-09	Establish and Communicate System Operating	FAC-010 FAC-011 FAC-014	Formal	9/29/17	11/13/17	Yes 11/13/17

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		Limits					
356	Project 2017-01	Modifications to BAL-003-1.1	SAR	Formal	11/2/17	12/1/17	Yes 12/1/17
357	Project 2016-02	Modifications to CIP Standard	CIP-012-1	Formal	10/27/17	12/11/17	Yes 12/11/17
358	Project 2016-02	Modifications to CIP Standard	Technical Rationale/Justification	Informal	11/20/17	12/11/17	Yes 12/11/17
359	Project 2017-03	FAC-008-3 Periodic Review	FAC-008-3	Formal	10/30/17	12/13/17	Yes 12/13/17
360	Project 2016-04	Modifications to PRC-025-1	PRC-025-1	Formal	10/30/17	12/13/17	Yes 12/13/17
361	Project 2017-07	Alignment with Registration	SAR	Formal	12/11/17	1/9/18	Yes 1/9/18
362	Project 2017-05	NUC-001-3	NUC-001-3	Formal	12/15/17	1/29/18	Yes 1/29/18
363	Project 2017-04	INT Periodic Review	INT-004-3.1 INT-006-4 INT-009-2.1 INT-010-2.1	Formal	1/10/18	2/23/18	Yes 2/23/18
364	Project 2017-07	Standards Alignment with Registration	Multiple Standards	Formal	2/1/18	3/2/18	Yes 3/2/18
365	Project 2017-02	Modifications to Personnel Performance, Training and Qualifications (PER) Standards	PER-003-1 PER-004-2	Formal	1/22/18	3/7/18	Yes 3/7/18
366	Project 2015-10	Single Points of Failure	TPL-001-5	Formal	2/23/18	4/23/18	Yes 4/23/18
367	Project 2018-01	Canadian-specific Revisions to TPL-007-2 SAR	TPL-007-2 SAR	Formal	3/30/18	4/30/18	Yes 4/30/18
368	Project 2016-02	Modifications to CIP Standard	CIP-002-6	Formal	3/16/18	4/30/18	Yes 4/30/18
369	Project 2016-02	Modifications to CIP Standard	CIP-012-1	Formal	3/16/18	4/30/18	Yes 4/30/18
370	Project 2016-02	Modifications to CIP Standard	Control Center Definition and Implementation	Formal	3/16/18	4/30/18	Yes 4/30/18
371	Standards Grading	2018 Periodic Review Standing Review Team	Standard Grading	Informal	5/14/18	6/28/18	Yes 6/28/18
372	Project 2016-02	Modifications to CIP Standard	CIP-012-1	Formal	5/18/18	7/3/18	Yes 7/2/18
373	SER	Standard Efficiency Review	SAR	Informal	6/7/18	7/10/18	Yes 7/10/18
374	Project 2016-02	Modifications to CIP Standard	CIP-002-5.1a SAR	Informal	6/14/18	7/13/18	Yes 7/13/18
375	Project 2016-02	Modifications to CIP Standard	CIP-003-7 SAR Order 843	Informal	6/14/18	7/13/18	Yes 7/13/18
376	SPM	Standards Processes Manual	SPM	Formal	6/25/18	8/9/18	Yes 8/9/18

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
377	Project 2018-01	Canadian-specific Revisions to TPL-007-2	TPL-007-2	Informal	8/10/18	9/6/18	Yes 9/6/18
378	Project 2018-02	Modifications to CIP-008 Cyber Security Incident Reporting SAR	CIP-008-5	Informal	8/10/18	9/10/18	Yes 9/10/18
379	Project 2015-10	Single Points of Failure	TPL-001-5	Formal	7/30/18	9/14/18	Yes 9/14/18
380	Functional Model Advisory Group	Functional Model Advisory Group	Functional Model Advisory Group	Informal	8/3/18	9/19/18	Yes 9/17/18
381	Project 2017-01	Modifications to BAL-003-1.1	BAL-003-1.1	Informal	9/6/18	9/20/18	Yes 9/20/18
382	SER	Standard Efficiency Review	SAR	Formal	8/28/18	9/26/18	Yes 9/26/18
383	Project 2016-02	Modifications to CIP Standards	CIP-002-6	Formal	8/23/18	10/9/18	Yes 10/9/18
384	Project 2016-02	Modifications to CIP Standards	CIP-003-8	Formal	8/23/18	10/9/18	Yes 10/9/18
385	Project 2015-09	Establish and Communicate System Operating Limits	FAC-010 FAC-011 FAC-014	Formal	8/24/18	10/17/18	Yes 10/17/18
386	Project 2018-02	Cyber Security – Incident Reporting and Response Planning	CIP-008-6	Formal	10/3/18	10/22/18	Yes 10/22/18
387	Project 2018-01	Canadian-specific Revisions to TPL-007-2	TPL-007-2	Formal	10/2/18	11/15/18	Yes 11/15/18
388	Project 2018-02	Cyber Security – Incident Reporting and Response Planning	CIP-008-6	Formal	11/15/18	11/29/18	Yes 11/29/18
389	Project 2016-02	Modifications to CIP Standards	Virtualization	Informal	11/2/18	12/18/18	Yes 12/18/18
390	Project 2017-01	Modifications to BAL-003-1.1	BAL-003-1.1	Formal	12/4/18	1/17/19	Yes 1/17/19
391	Project 2018-04	Modifications to PRC-024-2	PRC-024-2	Formal	12/19/18	1/18/19	Yes 1/18/19
392	Standard Efficiency Review	Standard Efficiency Review	SER Phase 2 Concepts Survey	Informal	2/22/19	3/22/19	Yes 3/22/19
393	Project 2019-01	Modifications to TPL-007-3	TPL-007-3	Informal	2/25/19	3/26/19	Yes 3/26/19
394	Project 2018-03	Standard Efficiency Review Retirements	FAC-008-4 INT-006-5 INT-009-3 IRO-002-6 PRC-004-6 TOP-001-5	Formal	2/27/19	4/12/19	Yes 4/12/19

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
			VAR-001-6 FAC-013-2 INT-004-3.1 INT-010-2.1 MOD-001-1a MOD-004-1 MOD-008-1 MOD-020-0 MOD-028-2 MOD-029-2a MOD-030-3 MOD-001-2				
395	Project 2019-02	BES Cyber System Information Access Management	CIP-004-6	Formal	3/28/19	4/26/19	Yes 4/26/19
396	Project 2018-04	Modifications to PRC-024-2	PRC-024-2	Formal	4/17/19	5/31/19	Yes 5/31/19
397	Project 2016-02	Modifications to CIP Standards	Virtualization White Paper	Informal	5/30/19	6/28/19	Yes 6/28/19
398	Project 2016-02	Modifications to CIP Standards	CIP-002-6	Formal	6/3/19	7/17/19	Yes 7/17/19
399	Project 2018-04	Modifications to PRC-024-2	PRC-024-2	Informal	6/27/19	7/26/19	Yes 7/26/19
400	Project 2019-03	Cyber Security Supply Chain Risks	CIP-005-6 CIP-010-3 CIP-013-1	Informal	7/2/19	8/1/19	Yes 8/1/19
401	SER	CIP SER	CIP Standards	Formal	7/3/19	8/26/19	Yes 8/26/19
402	Project 2019-04	Modifications to PRC-005-6	PRC-005-6 SAR	Formal	7/30/19	8/28/19	Yes 8/28/19
403	Project 2019-05	Modifications to PER-003-2	PER-003-2	Informal	8/1/19	8/30/19	Yes 8/30/19
404	Project 2016-02	Modifications to CIP Standards	CIP-005	Informal	8/9/19	9/26/19	Yes 9/26/19
405	EMP	Electromagnetic Pulses Task Force Draft Strategic Recommendation	EMP	Informal	8/30/19	9/30/19	Yes 9/30/19
406	Project 2018-04	Modifications to PRC-024-2	PRC-024-2	Formal	9/20/19	11/4/19	Yes 11/4/19
407	Project 2019-06	Cold Weather SAR	SAR	Formal	10/4/19	11/5/19	Yes 11/5/19
408	Project 201707	Standards Alignment with Registration	FAC-002-3 IRO-010-3 MOD-031-3 MOD-033-2 NUC-001-4 PRC-006-4 TOP-003-4	Formal	10/29/19	12/12/19	Yes 12/12/19
409	Project 2016-02	Modifications to CIP Standards	CIP-002-6	Formal	11/1/19	12/16/19	Yes 12/16/19
410	Project	Technical Rationale for Reliability	IRO-001-4 IRO-002-6	Informal	11/4/19	12/18/19	Yes 12/18/19

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		Standards	IRO-006-East-2 IRO-008-2 IRO-009-2 IRO-010-2 IRO-014-3 IRO-017-1 IRO-018-1(i)				
411	Project 2019-02	BES Cyber System Information Access Management	CIP-004-6	Formal	12/20/19	2/3/20	Yes and No 2/3/20
412	Project 2019-03	Cyber Security Supply Chain Risks	CIP-005-6 CIP-010-3 CIP-013-1	Formal	1/27/20	3/11/20	Yes and No 3/11/20
413	Project 2019-06	Cold Weather SAR	SAR	Formal	2/19/20	3/19/20	Yes 3/19/20
414	Project	Technical Rationale for Reliability Standards	IRO-001-4 IRO-002-6 IRO-006-East-2 IRO-008-2 IRO-009-2 IRO-010-2 IRO-014-3 IRO-017-1 IRO-018-1(i)	Informal	4/10/20	4/20/20	Yes 4/20/20
415	Project 2020-01	Modifications to MOD-032-1	MOD-032-1	Informal	3/24/20	4/24/20	Yes 4/24/20
416	Project 2020-02	Transmission-connected Resources SAR	MOD-025 MOD-026 MOD-027 PRC-019 PRC-024	Informal	3/30/20	5/13/20	Yes 5/13/20
417	Project 2019-06	Cold Weather SAR	SAR	Informal	4/22/20	5/21/20	Yes 5/21/20
418	SER	Operational Data Exchange Simplification SAR	SAR	Survey	3/12/20	5/27/20	Yes 5/28/20
419	Project 2020-03	Supply Chain Low Impact Revisions	SAR	Informal	4/3/20	6/3/20	Yes 6/3/20
420	Project 2020-04	Modifications to CIP-012	SAR	Informal	4/8/20	6/11/20	Yes 6/11/20
421	Project 2019-03	Cyber Security Supply Chain Risks	CIP-005-6 CIP-010-3 CIP-013-1	Formal	5/7/20	6/22/20	Yes 6/22/20
422	Project 2019-04	Modifications to PRC-005-6	PRC-005-6	Formal	6/2/20	7/8/20	Yes 7/8/20
423	Project 2015-09	Establish and Communicate System Operating Limits	CIP-014-3 FAC-003-5 FAC-011-4 FAC-013-3 FAC-014-3 PRC-002-3 PRC-026-2 TOP-001-6	Formal	6/19/20	8/3/20	Yes 8/3/20

RSC Meeting #21-2, Agenda Item 4.3: Comment History
(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
			IRO-008-3				
424	2021-2023	Reliability Standards Development Plan	Reliability Standards Development Plan	Informal	8/11/20	9/9/20	Yes 9/9/20
425	Project 2019-03	Cyber Security Supply Chain Risks	CIP-005-7 CIP-010-4 CIP-013-2	Formal	7/28/20	9/10/20	Yes 9/10/20
426	Project 2019-02	BES Cyber System Information Access Management	CIP-004-6	Formal	8/6/20	9/21/20	Abstention 9/17/20
427	Project 2015-09	Establish and Communicate System Operating Limits	CIP-014-3 FAC-003-5 FAC-011-4 FAC-013-3 FAC-014-3 PRC-002-3 PRC-026-2 TOP-001-6 IRO-008-3	Formal	10/23/20	12/7/20	Yes 12/7/20
428	Project 2020-05	Modifications to FAC-001-3 and FAC-002-2	SAR	Informal	11/12/20	12/11/20	Yes 12/11/20
429	Project 2018-03	Standard Efficiency Review Retirements	FAC-008-4	Formal	11/30/20	1/13/21	Yes 1/13/21
430	Project 2020-06	Verifications of Models and Data for Generators SAR	MOD-026-1 MOD-027-1	Formal	12/16/20	1/14/21	Yes 1/14/21
431	Project 2019-04	Modifications to PRC-005-6 SAR	PRC-005-6	Formal	1/14/21	2/26/21	Yes 2/26/21
432	Project 2019-06	Cold Weather	EOP-011-2 IRO-010-4 TOP-003-5	Formal	1/27/21	3/12/21	Yes 3/12/21
433	Project 2019-06	Cold Weather	EOP-011-2 IRO-010-4 TOP-003-5	Formal	4/2/21	4/26/21	Yes 4/26/21
434	Project 2017-01	Modifications to BAL-003 White Paper	BAL-003-2	Informal	3/29/21	4/27/21	Yes 4/27/21
435	2020 Periodic Review Standing Review Team	Standards Grading	Standards Grading	Formal	3/22/21	5/5/21	Yes 5/5/21
436	Project 2019-02	BES Cyber System Information Access Management	CIP-004-X CIP-011-X	Formal	3/25/21	5/10/21	Yes 5/10/21

RSC Meeting #21-2, Agenda Item 4.3: Comment History

(As of 5/10/2021)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted

Note: RSC past comment forms are posted on the NPCC Website under “[Standards - Regional Standards Comments](#).”

5/6/2021

Type	Document	Description	Comments	Status
Retirement	Directory#12	TFSS Retirement Recommendation	Posted for Member Comment Until June 12, 2021.	

NPCC Directory Executive Tracking Summary

Revised: 5/6/2021

	Document	Title	Responsible Task Force	Latest Version	Comments	Status
Directories						
	Directory #1	Design and Operation of the Bulk Power System	TFCP	Oct-15	TFCP has approved a Scope for the 2021 Directory #1 periodic review.	Joint CP-11/CO-7 Working Group Roster Established.
	Directory #2	Emergency Operations	TFCO	Jun-18		Revisions approved by Full Member Committee June 29, 2018.
	Directory #3	Maintenance Criteria for Bulk Power System Protection	TFSP	Jun-09		Directory#3 retired effective April 1st, 2015 coinciding with the enforcement date of PRC -005-2.
	Directory #4	Bulk Power System Protection Criteria	TFSP	Sep-15		Revisions approved by Full Member Committee January 30, 2020.
	Directory #5	Reserve	TFCO	Oct-12		Revisions approved by Full Member Committee September 27, 2019.
	Directory #6	Regional Reserve Sharing	TFCO	Apr-12		Revisions approved by Full Member Committee September 27, 2019.
	Directory #7	Remedial Action Schemes	TFSP	Dec-20		Revisions approved by Full Member Committee December 22, 2020
	Directory #8	System Restoration	TFCO	Sep-18		Revisions Approved by Full Member Committee September 25, 2018
	Directory #9	Verification of Generator Gross and Net Real Power Capability	TFCO	Dec-11		NPCC Full Member Committee approved retirement of D#9 and D#10 upon full enforcement of MOD-25-2. (July 1, 2019).
	Directory #10	Verification of Generator Gross and Net Reactive Power Capability	TFCO	Dec-11		See D#9.
	Directory#11	Disturbance Monitoring	TFSP	Oct-16	TFSP has begun its periodic review in November 2020.	Pending 1st Open Process Posting.
	Directory #12	Automatic UFLS	TFSS	Jul-13	TFSS has posted a retirement recommendation.	Directory#12 retirement recommendation posted for comment until June 12, 2021.
Criteria						
	A-10	Classification of BPS Elements	TFCP	Dec-09		Revisions Approved by Full Member Committee January 27, 2020.
Procedures						

NPCC Directory Criteria Clarifications

Revised: **5/6/2021**

/ be found at: <https://www.npcc.org/Standards/Directory%20Interpretations/Forms/Public%20List.aspx>

Line No.	Document	Title of Directory	Date Final	Task Force Review	Posted Open Process?	RCC Approval	Comments	Status
1	Directory #8 Interpretation	System Restoration	6/18/2012	TFCO	N/A	N/A	Interpretation on behalf of the NYSRC	Complete
2	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection	8/28/2012	TFSP	N/A	N/A	Interpretation on behalf of Bangor Hydro	Complete
3	Directory #3 Interpretation	Maintenance Criteria for Bulk Power System Protection	12/14/2012	TFSP	N/A	N/A	Interpretation on behalf of Con Ed	Complete
4	Directory #3 Interpretation	Maintenance Criteria for Bulk Power System Protection	2/15/2013	TFSP	N/A	N/A	Response Clarified - Interpretation on behalf of Acumen Engineered Solutions	Complete
5	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection	10/25/2013	TFSP	N/A	N/A	Interpretation on behalf of Hydro One Networks	Complete
6	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection	3/4/2015	TFSP	Yes	Yes	Interpretation on behalf of IESO-MACD	Complete.
7	Directory#8 Clarification	System Restoration	12/1/2015	TFCO	Yes	Yes	Clarification on Behalf of OPG.	Complete.
8	Directory#5 Clarification	Reserve	9/7/2016	TFCO	Yes	Yes	Clarification on Behalf of the NYISO.	Complete
9	Directory#1 Clarification	Design and Operation of the BPS	9/7/2016	TFCP	Yes	Yes	Clarification on Behalf of New Brunswick	Complete
10	Directory#4 Clarification	System Protection Criteria	12/2/2016	TFSP	Yes	Yes	Clarification on Behalf of Eversource	Complete
11	Directory #4 Clarification	System Protection Criteria	12/5/2017	TFSP	Yes	Yes	Clarification on Behalf of Eversource.	Complete
12	Directory#1 Clarification	Design and Operation of the BPS	5/30/2018	TFCP/TFCO	Yes	Yes	Clarification on Behalf of NYSRC	Complete
13	Directory #8 Clarification	System Restoration	9/8/2020	TFCO	Yes	Yes	Clarification on Behalf of OPG.	Complete

5/6/2021

Filing Period	Filing Due	Filing Submitted	Comments
October 1 to December 31, 2012	3/1/2013	3/1/2013	This filing is NPCC's initial quarterly filing covering the October 1 to December 31, 2012 period and covers the changes to the NPCC Criteria as a result of voting by the Full Members of NPCC.
January 1 to March 31, 2013	6/1/2013	N/A	No changes were made during the referenced period which required filing.
April 1 to June 30, 2013	9/1/2013	N/A	No changes were made during the referenced period which required filing.
July 1 to September 30, 2013	12/1/2013	11/25/2013	Revisions to D#7 and D#12 approved by the Full Members on 7/9/2013.
October 1 to December 31, 2013	3/1/2014	N/A	No changes were made during the referenced period which required filing.
January 1 to March 31, 2014	6/1/2014	N/A	No changes were made during the referenced period which required filing.
April 1 to June 30, 2014	9/1/2014	N/A	No changes were made during the referenced period which required filing.
July 1 to September 30, 2014	12/1/2014	N/A	No changes were made during the referenced period which required filing.
October 1 to December 31, 2014	3/1/2015	2/23/2015	(1) 10/15/14 NPCC Full Members approved retirement of D#3 effective 4/01/15 coinciding with enforcement date of PRC -005-2.
	3/1/2015	N/A	(2) 10/6/14 the RSC approved revisions to the Directory Manual which incorporated cost considerations into the Manual.
January 1st to March 31st 2015	6/1/2015	N/A	No changes were made during the referenced period which required filing.
April 1st to June 30th 2015	9/1/2015	N/A	No changes were made during the referenced period which required filing.
July 1 to September 30, 2015	12/1/2015	11/25/2015	Revisions to D#1 and D#4 approved by the Full Members on 9/30/2015.
October 1 to December 31, 2015	3/1/2016	N/A	No changes were made during the referenced period which required filing.
January 1st to March 31st, 2016	6/1/2016	N/A	No changes were made during the referenced period which required filing.
April 1 to June 30, 2016	9/1/2016	N/A	No changes were made during the referenced period which required filing.
July 1 to September 30, 2016	12/1/2016	N/A	No changes were made during the referenced period which required filing.
October 1 to December 31, 2016	3/1/2017	2/28/2017	Directory#11 approved by Full Members October 2016.
January 1st to March 31st 2017	6/1/2017	N/A	No changes were made during the referenced period which required filing.
April 1st to June 30th, 2017	9/1/2017	Will Not Be Filed.	Revisions to the A-01 Document approved by the Full Members on 4/21/2017.
July 1 to September 30, 2017	12/1/2017	2/28/2018	On August 3, 2017 NPCC Full Members approved retirement of Directories #9 and #10 effective July 1, 2019
October 1 to December 31, 2017	3/1/2018	2/28/2018	Revisions to D#8 approved by the Full Members on 10/06/2017.
January 1st to March 31st, 2018	6/1/2018	N/A	No changes were made during the referenced period which required filing.
April 1st to June 30th, 2018	9/1/2018	8/30/2018	Revisions to Directory #2 approved by the Full Members on 6/29/2018.
July 1 to September 30, 2018	12/1/2018	11/26/2018	Revisions to D#8 and Retirement of A-01 approved by the Full Members on 9/25/2018
October 1 to December 31, 2018	3/1/2019	N/A	No changes were made during the referenced period which required filing.

REGIONAL STANDARDS COMMITTEE

Chairman: Guy V. Zito
Assistant Vice President - Standards
Northeast Power Coordinating Council, Inc.
Tel. (212) 840-1070
Email: gzito@npcc.org

Co-Vice Chairman: Quintin Lee
Program Manager - Reliability Compliance
Eversource Energy
780 North Commercial Street
Manchester, NH 03101
Office: (603) 634-3579
Cell: (603) 315-9010
Email: quintin.lee@eversource.com

Co-Vice Chairman: Michael Jones
Manager, Reliability Standards and Policy
National Grid
40 Sylvan Road
Waltham, Massachusetts 02451
Tel. (781) 907-2404
Email: michael.jones@nationalgrid.com

Sector 1 - Transmission Owners

Hydro One Networks, Inc.

Primary

Paul Malozewski, P. Eng., MBA, PMP
Senior Manager – Reliability Standards and
Compliance Assurance
Tel. 416-345-5005
Email: paul.malozewski@hydroone.com

Alternate

Payam Farahbakhsh, M. Eng, P. Eng.
Senior Network Management Engineer –
Reliability Standards and Compliance Assurance
Tel. (416) 345-5484
Email: Payam.Farahbakhsh@HydroOne.com

Consolidated Edison Company of New York, Inc.

Primary

Deidre Altobell
Chief Engineer, Transmission Planning
4 Irving Place
New York, NY 10003
Tel. (212) 460-3968
Fax (212) 529-1130
Email: altobelld@coned.com

Alternate

Martin Paszek
Manager, System Performance
Tel. (212) 460-6415
Fax (212) 529-1130
Email: paszekm@coned.com

National Grid

Primary

John Hastings
Lead Analyst, Transmission Control Center – NY
7437 Henry Clay Blvd HCB-3
Liverpool, NY 13088
National Grid, US
Tel. (315) 460-4139
Email: John.Hastings2@nationalgrid.com

Alternate

New Brunswick Power Corporation

Primary

Nurul Abser
Engineer IV, Compliance
Tel. (506) 458-3964
Cell. (506) 238-3624
Email: NAbser@nbpower.com

Alternate

Rob Vance
Senior Engineer, Corporate Compliance
Tel. (506) 458-3922
Email: rob.vance@NBPower.com

The United Illuminating Company

Primary

Michele Tondalo
Lead Analyst – NERC Compliance (O&P)
180 Marsh Hill Road
Orange, Connecticut 06477
Tel. (203) 499-2542
Email: Michele.Tondalo@uinet.com

Alternate

Michele Shafer
Lead Analyst – NERC Compliance
18 Link Dr.
Binghamton, New York 13904
Tel. (585) 484-6453
Cell. (607) 624-5984
Email: mshafer@nyseg.com

Hydro-Quebec TransÉnergie and Equipment

Primary

Nicolas Turcotte
Manager – RC Regulatory Affairs and
Compliance Implementation and Regulatory
Compliance
2 Complexe Desjardins, 13th floor, East Tower
Montréal, Québec, Canada H5B 1H7
Tel. (514) 798-1223
Ext :8795182
Email: turcotte.nicolas@hydro.qc.ca

Alternate

Stéphane Desbiens
Director – Reliability Standards & Regulatory
Compliance
2 Complexe Desjardins, 13th floor, East Tower
Montreal, Québec, Canada H5B 1H7
Tel. (514) 289-4435
Email: Desbiens.Stephane@hydro.qc.ca

Orange & Rockland Utilities, Inc.

Primary

Nick Kowalczyk
Chief System Operator
390 West Route 59
Spring Valley NY 10977
Tel. (845) 577-3796
Email: kowalczykn@oru.com

Alternate

Susmit Patel
Section Manager – Substation & Transmission
Engineering
Orange and Rockland Utilities Inc.
390 West Route 59
Spring Valley NY 10977
845-577-3203
Email: patels@oru.com

Eversource Energy

Primary

Quintin Lee
Program Manager - Reliability Compliance
Eversource Energy
780 North Commercial Street
Manchester, NH 03101
Office: (603) 634-3579
Cell: (603) 315-9010
Email: quintin.lee@eversource.com

Alternate

Sharon Flannery
Program Manager – Reliability Compliance
Eversource Energy
107 Selden Street
Berlin, CT
Office: (860) 665-5247
Cell: (860) 402-9157
Email: sharon.flannery@eversource.com

Central Hudson Gas & Electric

Primary

Michael Ridolfino
Engineer – Reliability Compliance
Office: (845) 486-5674
Cell: (845) 750-0896
Email: mridolfino@cenhud.com

Alternate

Sector (2) - Reliability Coordinators

New York Independent System Operator

Primary

James (Jim) Grant
Senior Reliability Engineer
Tel. (518) 356-6128
Email: jgrant@nyiso.com

Alternate

Gregory A. Campoli
Manager, Reliability Compliance & Industry
Affairs
Tel. (518) 356-6159
Email: gcampoli@nyiso.com

ISO New England, Inc.

Primary

John Pearson
Technical Manager
Tel. (413) 540-4260
Email: jpearson@iso-ne.com

Alternate

Kathleen M. Goodman
Senior Operations Compliance Coordinator
Tel. (413) 535-4111
Email: kgoodman@iso-ne.com

Independent Electricity System Operator

Primary

Helen Lainis
Senior Engineer/Technical Officer
Tel. (905) 855-4106
Email: helen.lainis@ieso.ca

Alternate

Sean Lagan
Compliance Analyst
Tel. (905) 855-6283
Email: sean.lagan@ieso.ca

Hydro-Quebec TransÉnergie and Equipment

Primary

Chantal Mazza
Reliability Standards Advisor III
2 Complexe Desjardins, 13th floor, East Tower
Montréal, Québec, Canada H5B 1H7
Tel. (514) 798-1223 Ext. 8795499
Email: mazza.chantal@hydro.qc.ca

Alternate

Junji Yamaguchi
Manager - Reliability Standards and Operating
Procedures
2 Complexe Desjardins, 13th floor, East Tower
Montreal, Québec, Canada H5B 1H7
Tel. (514) 289-2211 Ext. 2667
Email: Yamaguchi.junji@hydro.qc.ca

New Brunswick Power Corporation

Primary

Randy MacDonald
Director, Corporate Compliance
Tel. (506) 458-4653
Cell. (506) 470-3536
Email: RaMacDonald@NBPower.com

Alternate

Tim Hicks
Document & Compliance Coordinator
Tel. (506) 458-6511
Cell. (506) 238-3851
Email: Tim.Hicks@nbpower.com

Sector (3) - Transmission Dependent Utilities (“TDUs”); Distribution Companies and Load-Serving Entities (“LSEs”)

Consolidated Edison Company of New York, Inc.

Primary

Dermot Smyth
Senior Engineer
Tel. (212) 460-4093
Fax (212) 529-1130
Email: smythd@coned.com

Alternate

Lincoln Burton
Senior Engineer
Tel. (646) 660-3899
Fax (212) 529-1130
Email: burtonl@coned.com

National Grid

Primary

Michael Jones
Manager, Reliability Standards and Policy
40 Sylvan Road
Waltham, Massachusetts 02451
Tel. (781) 907-2404
Email: michael.jones@nationalgrid.com

Alternate

Orange & Rockland Utilities, Inc.

Primary

David Burke
Senior Specialist - Compliance
Tel. (845) 577-2841
Email: burkeda@oru.com

Alternate

Ben Wu
Principal Engineer
Transmission & Substation Engineering
Tel. (845) 577-3713
Email: wub@oru.com

Sector (4) - Generator Owners

Consolidated Edison Company of New York, Inc.

Primary

Peter Yost
Manager, Standards & Compliance
Tel. (212) 460-2889
Fax (212) 529-1130
Email: yostp@coned.com

Alternate

Avani Pandya
Engineer
Fax (212) 529-1130
Email: pandyaa@coned.com

New York Power Authority

Primary

Salvatore Spagnolo
Program Manager, Reliability Standards & Compliance
Tel. (914) 390-8224
Mob. (347) 992-7015
Email: Salvatore.Spagnolo@nypa.gov

Alternate

Dominion Energy Services, Inc.

Primary

Sean Bodkin
NERC Compliance Policy Manager
Dominion Energy Services, Inc.
Tel. (804) 771-8429, tie line 8-786-8429
Cell: (804) 292-5721
Email: Sean.Bodkin@dominionenergy.com

Alternate

Connie Lowe
Regulatory and Market Policy Manager
Dominion Energy Services, Inc.
Tel. (804) 771-4447, tie 8-736-4447
Cell: 804-239-3201
Email: connie.lowe@dominionenergy.com

Ontario Power Generation, Inc.

Primary

Mike Cooke
Director – Reliability Compliance
Tel. (416) 592-6089
Cell: (905) 483-5520
Email: mike.cooke@opg.com

Alternate

David Kwan
Senior Regulatory Analyst
Tel. (416) 592-6369
Email: david.kwan@opg.com

Alternate

Constantin Chitescu
Regulatory Analyst
Tel. (416) 592-6055
Email: constantin.chitescu@opg.com

NextEra Energy, LLC

Primary

Silvia Parada Mitchell
Senior Director, Reliability Standards & Compliance
Tel. (561) 904-3767
Email: silvia.parada.mitchell@fpl.com

Alternate

Summer Esquerre
Director Reliability Standards & Compliance
Tel. (561) 904-3765
Email: summer.esquerre@fpl.com

Entergy Services, Inc

Primary

Glen Smith
NERC Compliance
Entergy Services, Inc
440 Hamilton Avenue
White Plains, NY 10601
914-272-3513
Email: gsmith@entergy.com

Alternate

Joel Plessinger
Manager, Operations & Planning Standards
NERC Compliance
Tel: (281)297-3644
Email: jplessi@entergy.com

PSEG

Primary

Sean Cavote
Director NERC Compliance
PSEG Law Department
80 Park Plaza, P3
Newark, NJ 07102-4194
973-430-5310
Email: sean.cavote@pseg.com

Alternate

Tim Kucey
Manager NERC Compliance
80 Park Plaza, P3
Newark, NJ 07102-4194
908-412-3078
Email: Timothy.Kucey@PSEG.com

Sector (5) - Marketers, Brokers and Aggregators

Consolidated Edison Company of New York, Inc.

Primary

Cristhian Godoy
Senior Engineer
4 Irving Place, New York, NY 10003
Tel. (917) 612-6364
Fax (212) 529-1130
Email: godoyc@coned.com

Alternate

Qinling Zheng
Engineer
Tel. (212) 460-2790
Fax (212) 529-1130
Email: zhengq@ConEd.com

Utility Services, Inc.

Primary

Brian Robinson
COO
Tel. (802) 241-1400
Email: brian.robinson@utilitysvcs.com

Alternate

Brian Evans-Mongeon
President/CEO
Tel. (802) 241-1400
Email: brian.evans-mongeon@utilitysvcs.com

Sector (6) – State and Provincial Regulatory and/or Governmental Authorities

New York Power Authority

Primary

Shivaz Chopra
Director, Reliability Standards & Compliance
Tel. (914) 681-6828
Tel. (914) 391-6839
Email: shivaz.chopra@nypa.gov

Alternate

Erick Barrios
Engineer, Reliability Standards & Compliance
Tel. (914) 681-6781
Tel. (914) 506-2152
Email: Erick.Barrios@nypa.gov

New York State Department of Public Service

Primary

Vijay Puran
Utility Supervisor, Bulk Electric Systems
Tel. (518) 486-5948
Email: vijay.puran@dps.ny.gov

Alternate

Jerry Ancona
Senior Engineer
Tel. (315) 448-7300
Email: Jerry.Ancona@dps.ny.gov

Sector 7 – Sub-Regional Reliability Councils, Customers and Other Regional Entities and Interested Entities

New York State Reliability Council, LLC

Primary

Alan Adamson
Independent Consultant
2104 Braxton Street
Clermont, FL 34711
Tel. (352) 989-4653
Email: aadamson@nycap.rr.com

Alternate

Independent

Primary

David Kiguel
Independent Consultant
Toronto, Canada
Email: David.kiguel@outlook.com

Alternate

AESI, Inc.

Primary

Joel Charlebois
Vice President, Regulatory Compliance
Tel. (770) 870-1630 x 236
Cell: (718) 419-4012
Email: JoelC@aesi-inc.com

Alternate